ACTION RESEARCH PROJECT REPORT

Project no: ARP-004

Study of the permissions sought by Mobile Applications

Kshitij Bathla
Scientist -C
Electronics & IT Department
Bureau of Indian Standards

Table of contents

1. Background

Mobile Application (generally known as mobile app) is the software program that is specifically run on mobile device. Many organizations be it in private sector or public sector offers its services through its Mobile app and users are encouraged to use mobile apps. These mobile apps collect various types of data that may or may not be relevant for them. Data is the commodity in the IT world and data collected by these apps can be used for various purposes like profiling for targeted advertising etc.

As per joint study by Associated Chambers of Commerce and Industry of India and PwC, in **2017** there were approximately **one billion mobile phone users** and out of these 468 million were smartphone users. The number of smartphone users in India is expected to rise by 84% to 859 million by 2022 from 468 million in 2017.

As per the report 'Digital India - Technology to Transform a Connection Nation' by McKinsey Global Institute, Indians have **1.2 billion mobile phone subscriptions** and **downloaded more apps -- 12.3 billion in 2018** -- than residents of any other country except China.

Most of the mobile application can be used without paying any subscription fee and as there is saying "Nothing comes for free" so what is the hidden fee. It is the data collected by app. On an average every smartphone user has 20 mobile applications installed on their device and if even one out of these applications is collecting data without the knowledge of user then that is privacy breach.

At International level and at National level Standards are being formulated to address the general privacy concerns. Outcome of this study may provide suggestions to mitigate privacy concerns specific to mobile applications that may be addition to the exiting standards or a new standard specific for mobile applications.

2. Objective

To Study the various permissions sought by various mobile applications in relation to the function of the mobile applications.

The study was limited to android based application used in smartphones.

The intent of the study

- to analyze the various types of permissions sought by different types of mobile applications
- to provide recommendations based on the findings of the study.

Applications studied during this study have been selected randomly and there is no intention to target any specific application. Objective of study is only to provide recommendation which could help applications developers and mobile phone manufacturers to ensure data privacy and help user in providing better informed consent.

3. Research Methodology

- Downloading the mobile application randomly on the mobile phone.
- Use the application
- Analysing the permissions sought by mobile app and understanding the relation between permission and functioning of app.

4. Introduction

Mobile Application (generally known as mobile app) is the software program that is specifically run on mobile device. Mobile application could be downloaded in mobile like from play store or it could be a pre-installed application. Applications which are downloaded from play store are known as Third party applications.

Camera, calendar are examples of pre-installed applications. Amazon, Flipkart, BHIM, GPay are examples of third-party applications. Both types of applications have been studied during this study.

5. Categories of Permissions

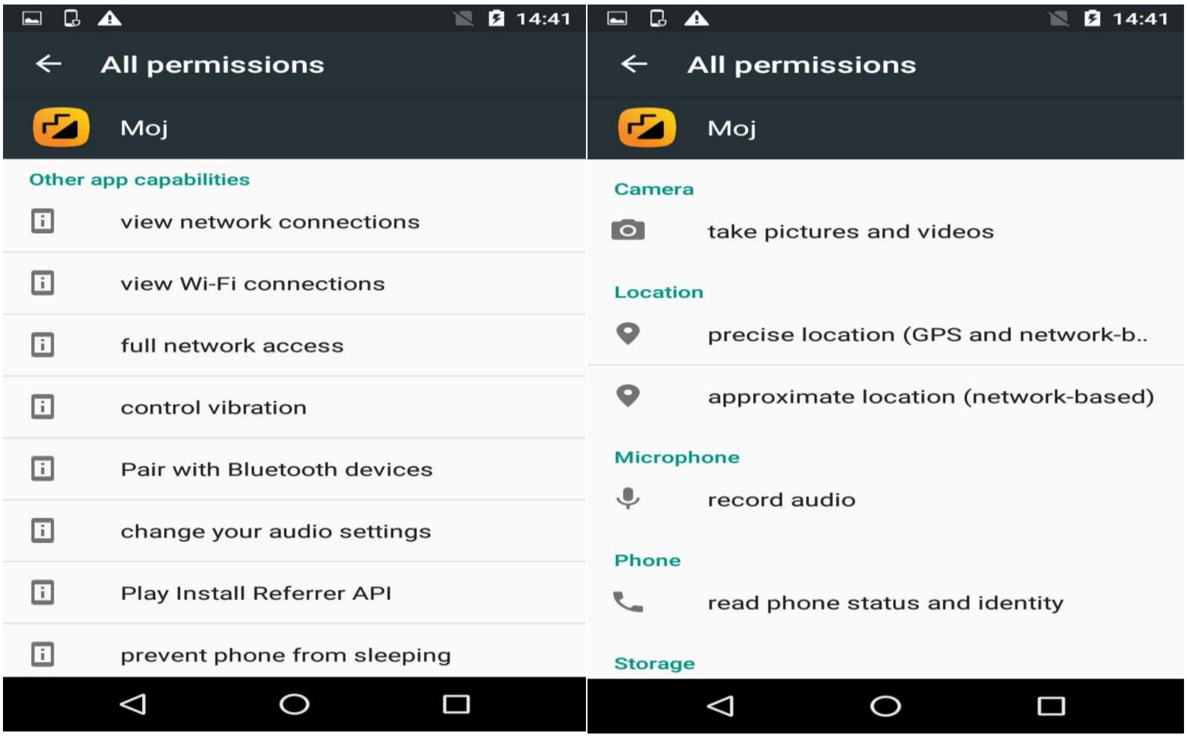
Mobile application is a software that run using hardware and software capabilities/resources of the mobile phone. It has been found that Mobile applications utilize hardware and software capabilities of the mobile phone in following two ways.

a) First is by **specifically seeking permission** from the mobile user to use specific resource/capability of the mobile phone like use of location, microphone etc. [Refer Screenshot 1 & 2].

These types of permissions have been mentioned in this study as **Type 1 Permissions.**

b) Second is classified as '**other app capabilities'**. For these capabilities' app may or may not **seek specific permissions** from the Mobile phone user like 'view network connections', 'control vibrations', 'pair with Bluetooth devices' etc. [Refer Screenshot 1 & 2].

For this study 'other app capabilities' have been mentioned as **Type 2 Permissions.**



All permissions

Moj

Other app capabilities

- view network connections
- view Wi-Fi connections
- full network access
- control vibration
- Pair with Bluetooth devices
- change your audio settings
- Play Install Referrer API
- prevent phone from sleeping

All permissions

Moj

Camera

- take pictures and videos

Location

- precise location (GPS and network-b..
- approximate location (network-based)

Microphone

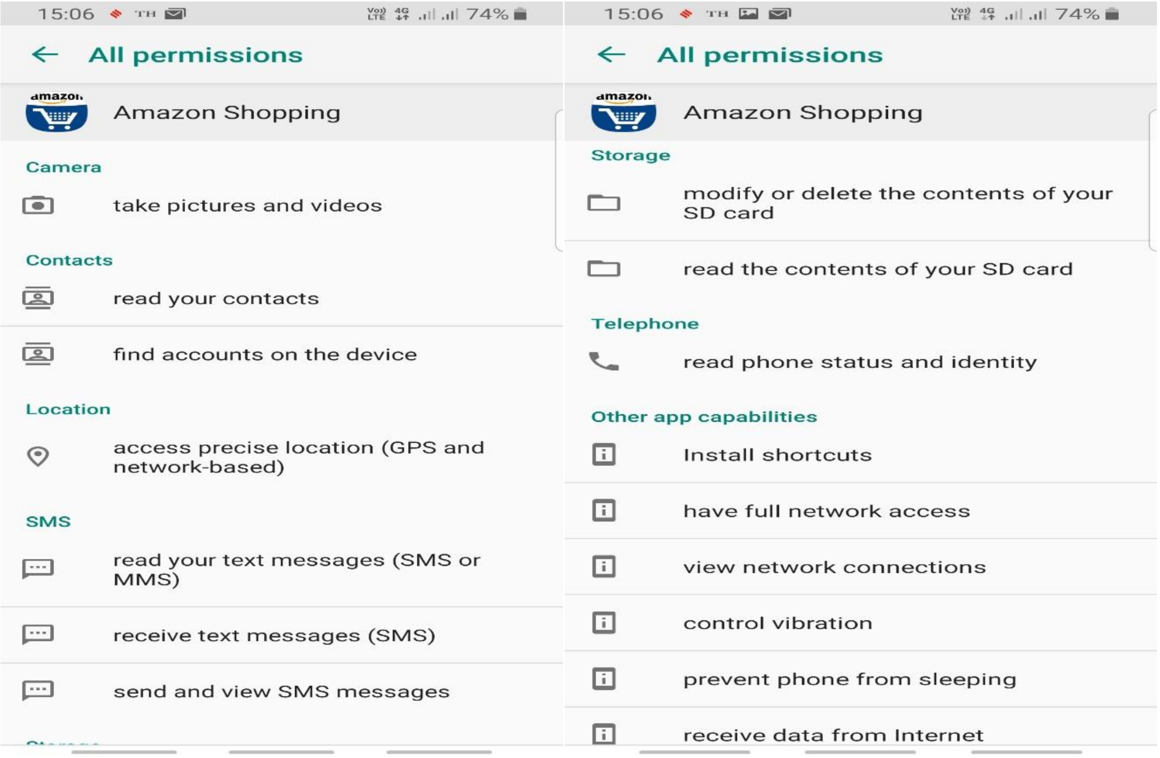
- record audio

Phone

- read phone status and identity

Storage

Screenshot 1



All permissions

Amazon Shopping

Camera

- take pictures and videos

Contacts

- read your contacts
- find accounts on the device

Location

- access precise location (GPS and network-based)

SMS

- read your text messages (SMS or MMS)
- receive text messages (SMS)
- send and view SMS messages

All permissions

Amazon Shopping

Storage

- modify or delete the contents of your SD card
- read the contents of your SD card

Telephone

- read phone status and identity

Other app capabilities

- Install shortcuts
- have full network access
- view network connections
- control vibration
- prevent phone from sleeping
- receive data from Internet

Screenshot 2

6 Details of various permissions

6.1 During the study it has been found that following are Type 1 permissions:

i. Camera
ii. Call logs
iii. Location
iv. SMS
v. Storage
vi. Contacts
vii. Microphone
viii. Calendar
ix. Telephone/Phone

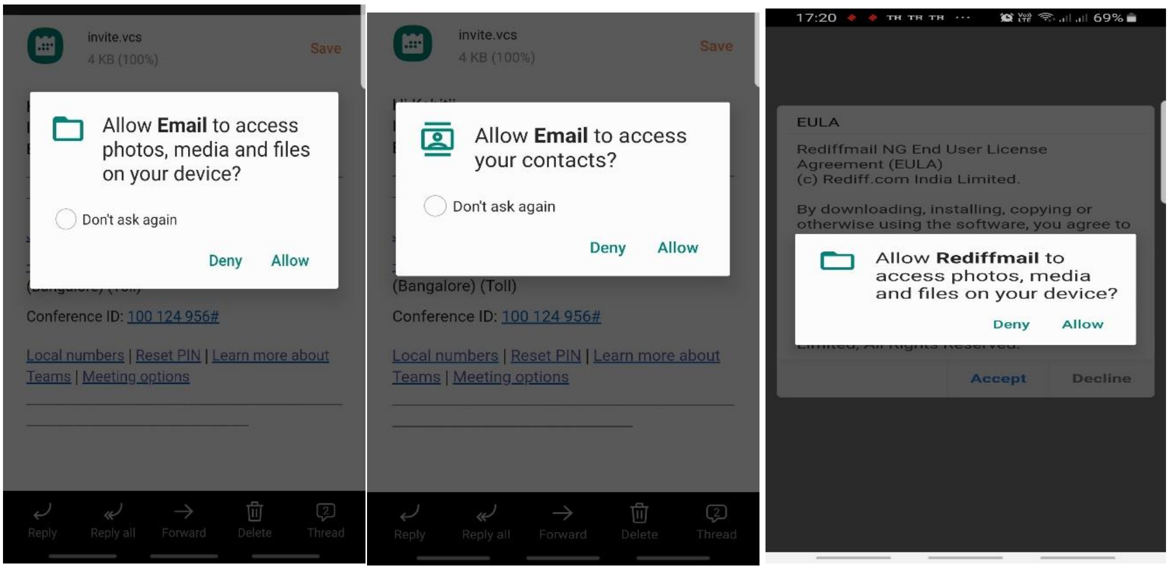
6.2 During the study it has been found that following are Type 2 permissions:

i. Pair with Bluetooth devices
ii. Run at startup
iii. Receive data from the internet
iv. view network connections
v. control vibrations
vi. Prevent phone from sleeping
vii. Have full network access
viii. Use biometric hardware
ix. Use fingerprint hardware
x. View wi-fi connections
xi. Send sticky broadcast
xii. Install shortcuts

Lists given at 6.1 and 6.2 are not exhaustive but indication of most commonly found permissions.

6.3Purpose of permissions

6.3.1 Ideally all mobile applications should inform the purpose of all the permissions sought by them and from the study it has been found that most of the applications seek permissions from the user however the **permission sought is not specific and is too generic**. For example, refer Screenshot 3 & 4.



invite.vcs
4 KB (100%)

Allow **Email** to access photos, media and files on your device?

○ Don't ask again

Conference ID: 100 124 956#

Local numbers | Reset PIN | Learn more about Teams | Meeting options

invite.vcs
4 KB (100%)

Allow **Email** to access your contacts?

○ Don't ask again

(Bangalore) (Toll)

Conference ID: 100 124 956#

Local numbers | Reset PIN | Learn more about Teams | Meeting options

17:20 69%

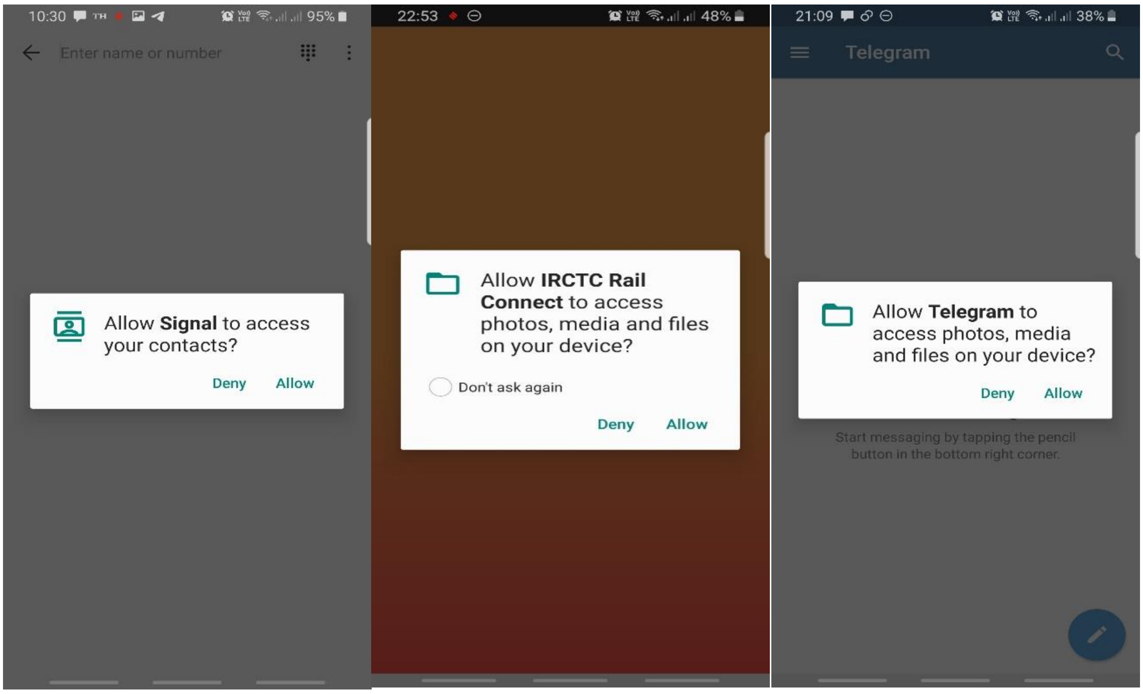
EULA

Rediffmail NG End User License Agreement (EULA)
(c) Rediff.com India Limited.

By downloading, installing, copying or otherwise using the software, you agree to

Allow **Rediffmail** to access photos, media and files on your device?

Screenshot 3



10:30 95%

Enter name or number

Allow **Signal** to access your contacts?

22:53 48%

Allow **IRCTC Rail Connect** to access photos, media and files on your device?

○ Don't ask again

21:09 38%

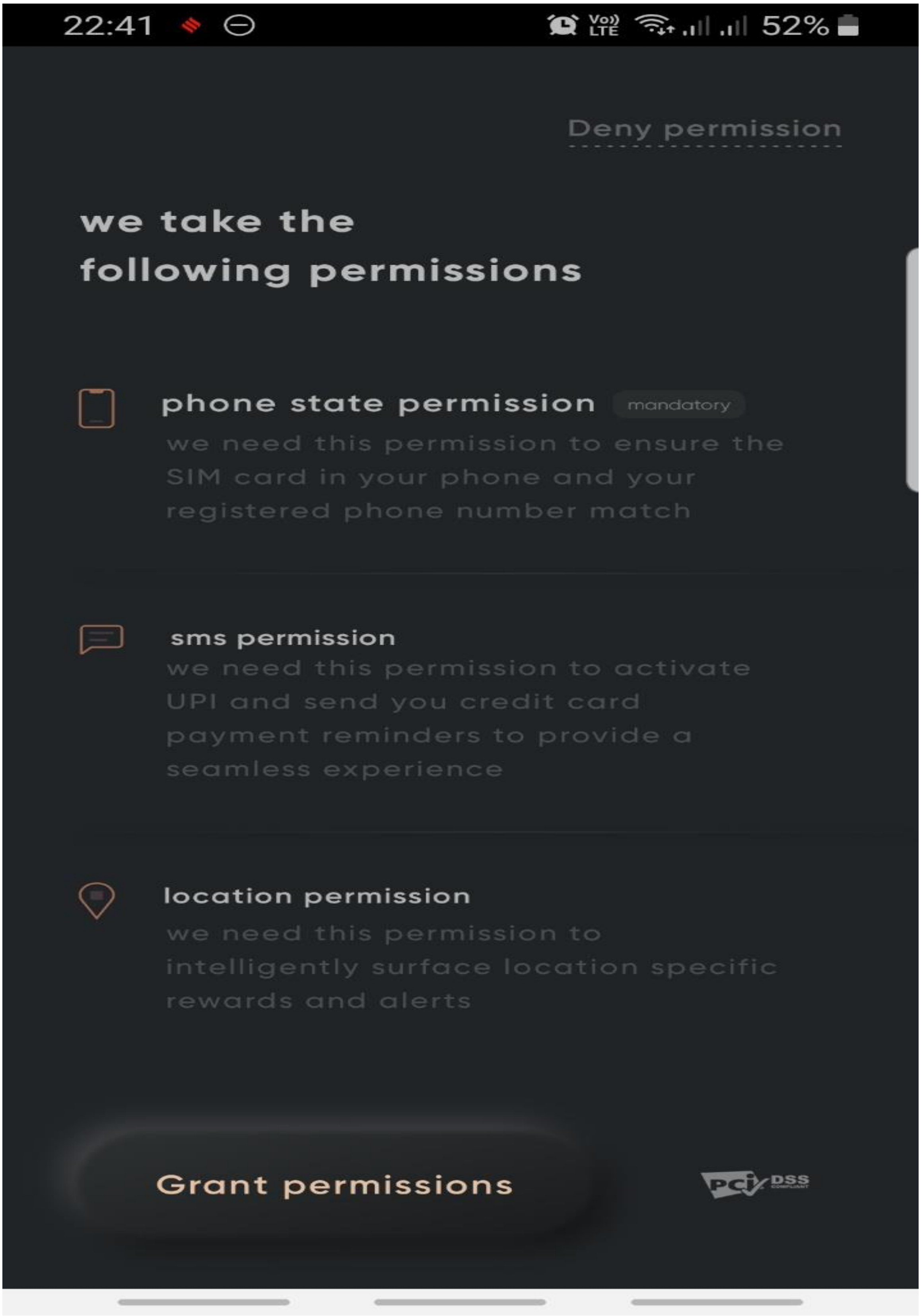
Telegram

Allow **Telegram** to access photos, media and files on your device?

Start messaging by tapping the pencil button in the bottom right corner.

Screenshot 4

From the above examples it is evident that specific purpose of the permission is not clear. For better understanding of the user, transparency and informed consent specific purpose of permissions should be informed to the user. Some of the applications have been found informing specific purpose for example refer screenshot 5 & 6.



we take the following permissions

phone state permission mandatory

we need this permission to ensure the SIM card in your phone and your registered phone number match

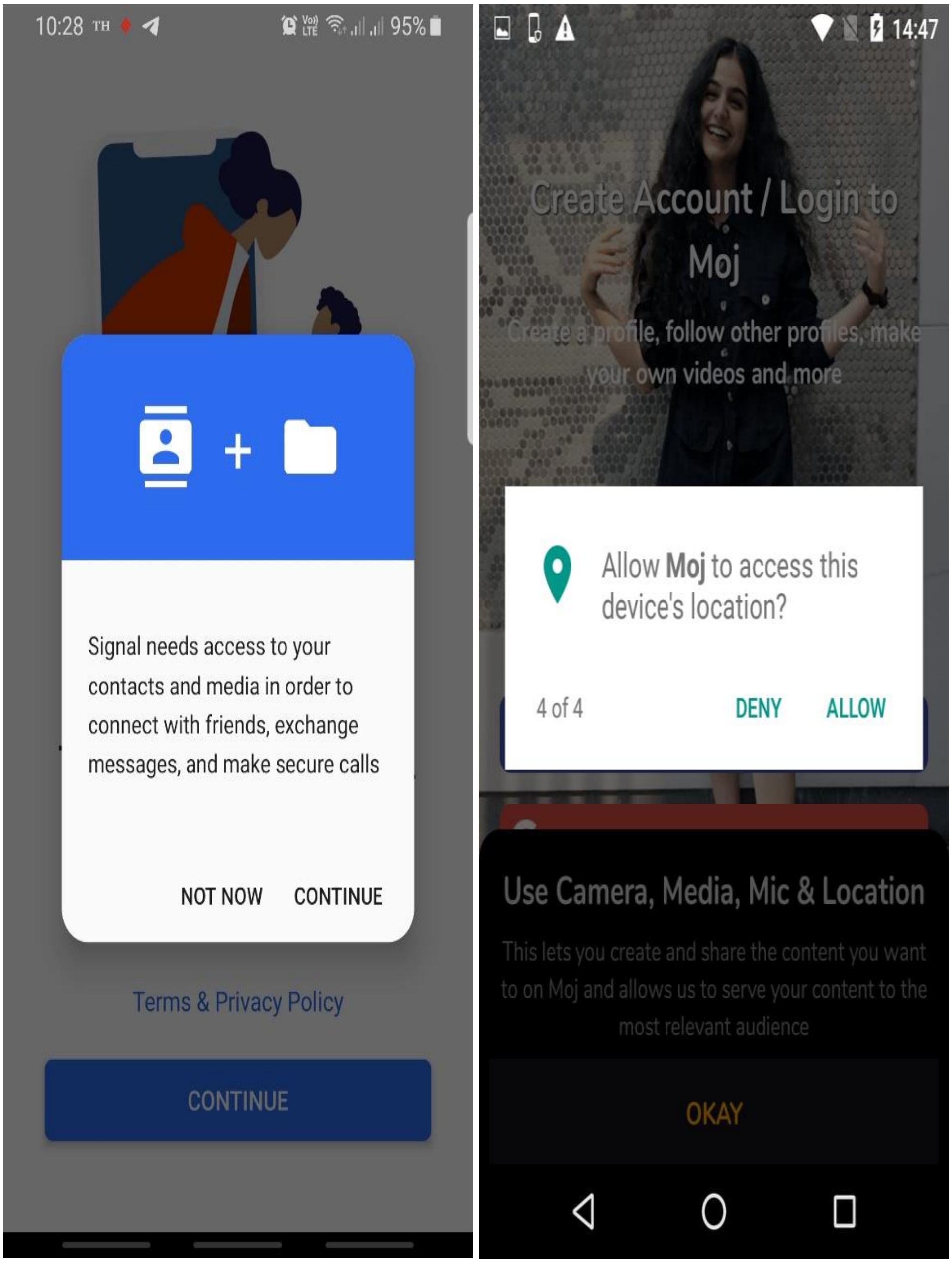
sms permission

we need this permission to activate UPI and send you credit card payment reminders to provide a seamless experience

location permission

we need this permission to intelligently surface location specific rewards and alerts

Screenshot 5



10:28 TH 95%

Signal needs access to your contacts and media in order to connect with friends, exchange messages, and make secure calls

NOT NOW CONTINUE

Terms & Privacy Policy

CONTINUE

14:47

Create Account / Login to Moj

Create a profile, follow other profiles, make your own videos and more

Allow **Moj** to access this device's location?

4 of 4 DENY ALLOW

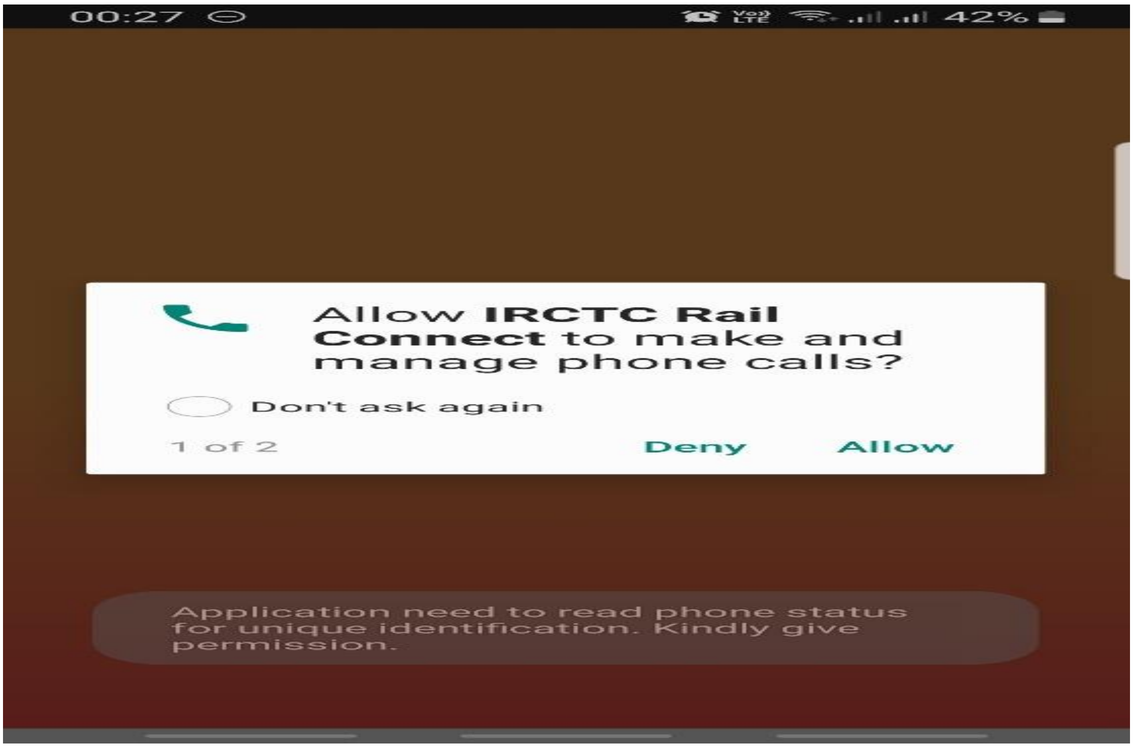
Use Camera, Media, Mic & Location

This lets you create and share the content you want to on Moj and allows us to serve your content to the most relevant audience

OKAY

Screenshot 6

Some instances were found where specific reason for permission was informed only after denying the permission. For example, refer screenshot 7&8

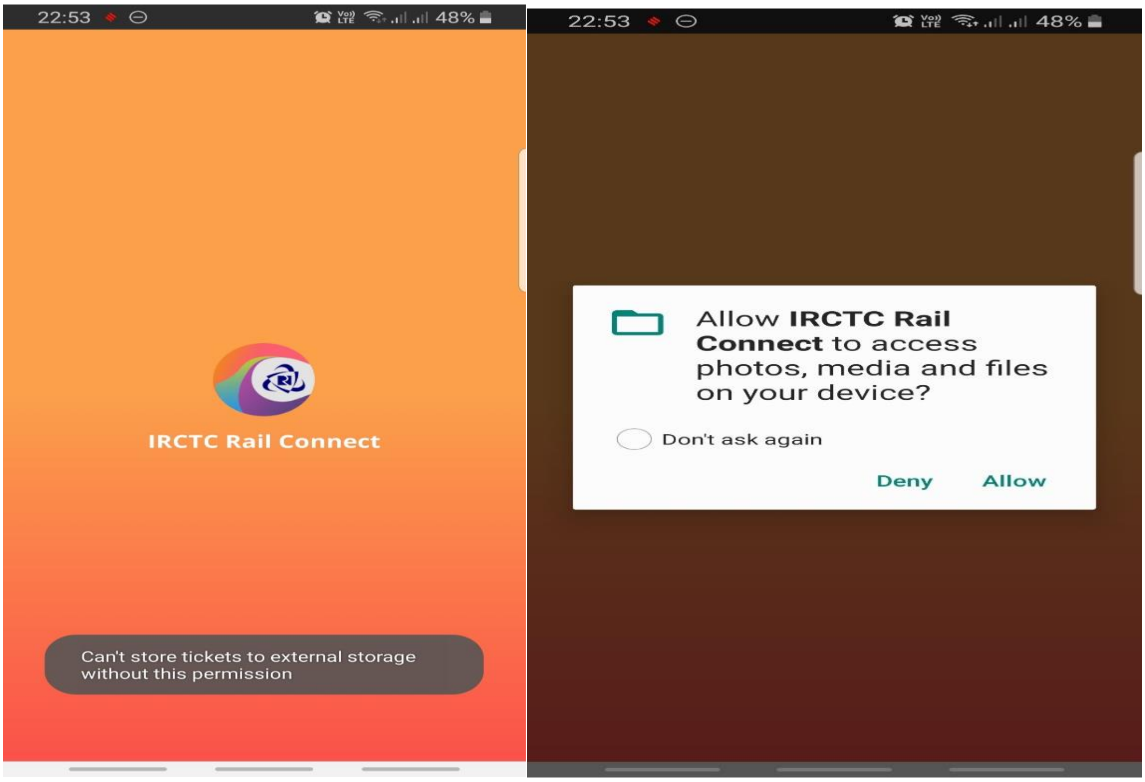


Allow **IRCTC Rail Connect** to make and manage phone calls?

○ Don't ask again

Application need to read phone status for unique identification. Kindly give permission.

Screenshot 7



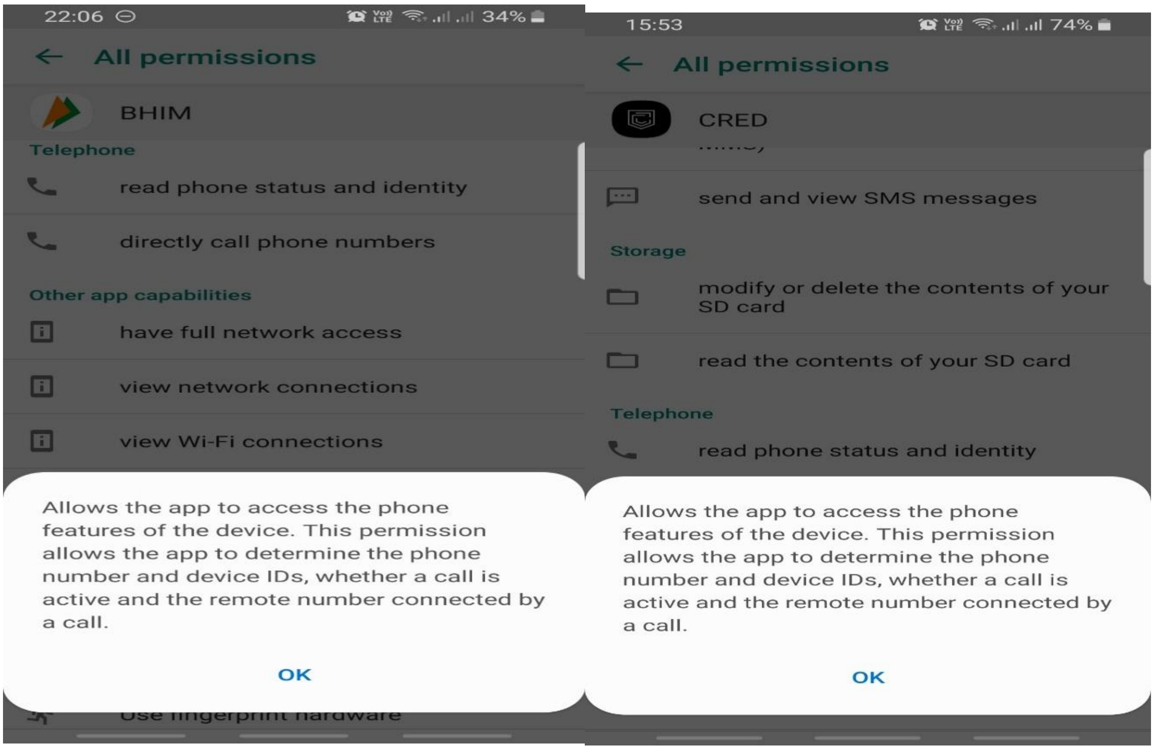
Can't store tickets to external storage without this permission

Allow **IRCTC Rail Connect** to access photos, media and files on your device?

○ Don't ask again

Screenshot 8

6.3.2 Examples of purpose of permission shown at 6.3.1 are by specific app, apart from this Android system also provides a description of the purpose of the permission and this is also generic and irrespective of the function of the application. For example, refer screenshot 9



Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active and the remote number connected by a call.

OK
Use fingerprint hardware
15:53
74%
All permissions
CRED
send and view SMS messages
Storage
modify or delete the contents of your SD card
read the contents of your SD card
Telephone
read phone status and identity

Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active and the remote number connected by a call.

Screenshot 9

Description of Type 1 and Type 2 permissions as per Android system irrespective of the Mobile application is given Table 1 and Table 2 respectively:

Table 1

Permission	**Description as per Android system irrespective of the Mobile application**
Camera	This app can take pictures and record videos using the camera at any time
Call logs	This app can read your call history
Location - Access approximate location (network-based) only in foreground	This app can get your location based on network sources such as cell towers and Wi-Fi networks, but only when the app is in the foreground. These location services must be turned on and available on your phone for the app to be able to use them.
Location - Access precise location only in the foreground	This app can get your exact location only when it is in the foreground. These location services must be turned on and available on your phone for the app to be able to use them. This may increase battery consumption.

SMS - Receive text messages (SMS)	Allows the app to receive and process SMS messages. This means the app could monitor or delete messages sent to your devices without showing them to you.
SMS - Send and view SMS messages	Allows the app to send SMS messages. This may result in unexpected charges. Malicious apps may cost you money by sending messages without your confirmation.
SMS - Read your text messages (SMS or MMS)	This app can read all SMS (TEXT) messages stored on your phone.
Storage - Modify or delete the contents of your shared storage	Allows the app to write the contents of your shared storage.
Storage - Read the contents of your shared storage	Allows the app to read the contents of your shared storage.
Contacts- read your contacts	Allows the app to read data about your contacts stored on your phone, including the frequency with which you have called, Emails or communicated in other ways with specific individuals. This permission allows apps to save your contacts data and malicious apps may share content data without your knowledge.
Contacts Find accounts on the devices	Allows the app to get the list of accounts known by the phone. This may include any accounts created by applications you have installed.
Microphone (audio recording)	Allows the app to record audio with the microphone. This app can record audio using the microphone at any time.
Calendar	This app can read all calendar events stored on your phone and share or save your calendar data.
Telephone/Phone -read phone status and identity	Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs whether a call is active and the remote number connected by a call.
Telephone/Phone - read phone numbers	Allows the app to access the phone numbers of the device
Telephone/Phone – directly call phone numbers	Allows the app to call phone numbers without your intervention. This may result in unexpected charges or calls. Note that this doesn’t allow the app to call emergency numbers. Malicious apps may cost you money by making calls without your confirmation.

Table 2

Other app capabilities	**Description as per Android system irrespective of the Mobile application**
Pair with Bluetooth devices	Allows the app to view the configuration of the Bluetooth on the phone, and to make and accept connections with paired devices.
Run at startup	Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the phone and allow the app to slow down the overall phone by always running.

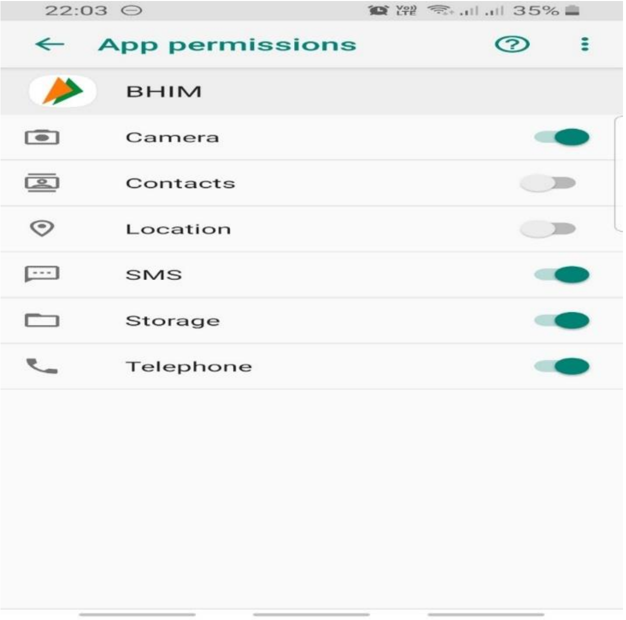
Receive data from the internet	Allows apps to accept cloud to device messages sent by the apps service. Using this service will incur data usage. Malicious apps could cause excess data usage.
view network connections	Allows the app to view information about network connections such as which networks exist and are connected.
control vibrations	Allows the app to control the vibrator.
Prevent phone from sleeping	Allows the app to prevent the phone from going to sleep.
Have full network access	Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.
Use biometric hardware	Allows the app to use biometric hardware for authentication.
Use fingerprint hardware	Allows the app to use fingerprint hardware for authentication.
View Wi-Fi connections	Allows the app to view information about Wi-Fi networking such as whether Wi-Fi is enabled and name of connected Wi-Fi devices.
Send sticky broadcast	Allows the app to send sticky broadcasts which remind after the broadcast ends. Excessive use may make the phone slow or unstable by causing it to use too much memory.
Install shortcuts	Allows an application to add home screen shortcuts without user intervention.

From the above study it is clear that reason given by Android OS is too broad and does not clearly convey the actual reason why the permission is required and even description provided by mobile application is not specific.

6.4Requirement of permissions with respect to function of application

It has been found that not all Type 1 permissions sought are required for basic intended function of application. For example, refer case 1.

Case 1:



22:03 35%

App permissions

BHIM

Camera ●

Contacts ○

Location ○

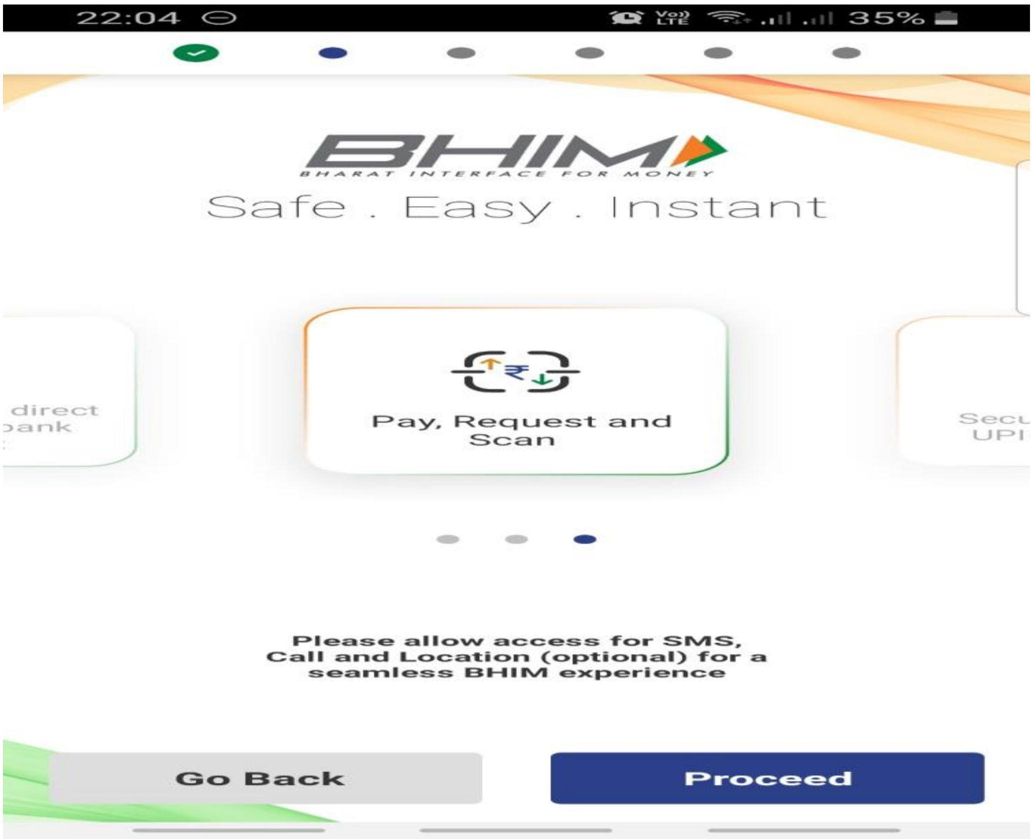
SMS ●

Storage ●

Telephone ●

Screenshot 10

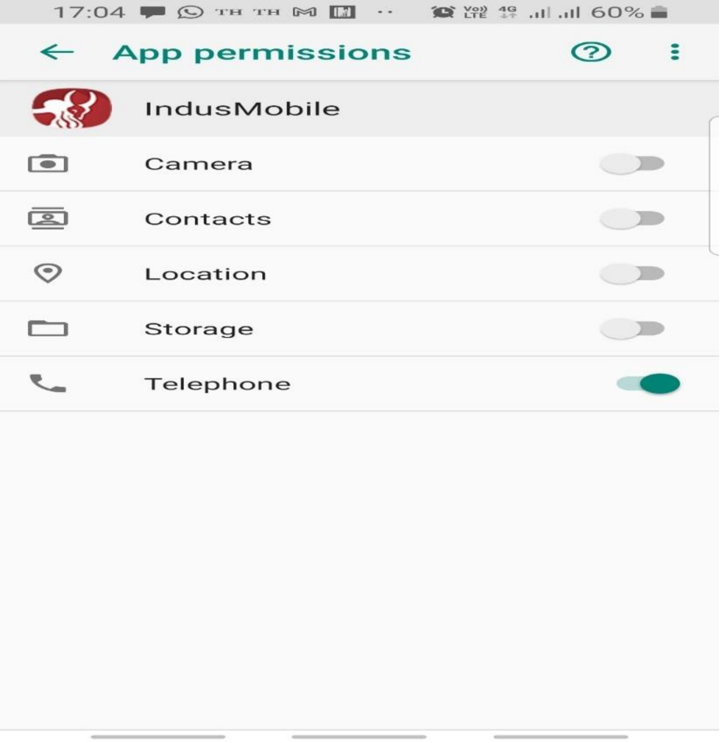
Screenshot 10 shows the case where most of the permissions sought by the app have been permitted. If we don't give permissions and application is opened for use then app behaves as displayed in **screenshot 11**. Screenshot 11 shows Application is informing the permissions which are essentially required and which are optional.



Please allow access for SMS, Call and Location (optional) for a seamless BHIM experience

Screenshot 11

Case 2:



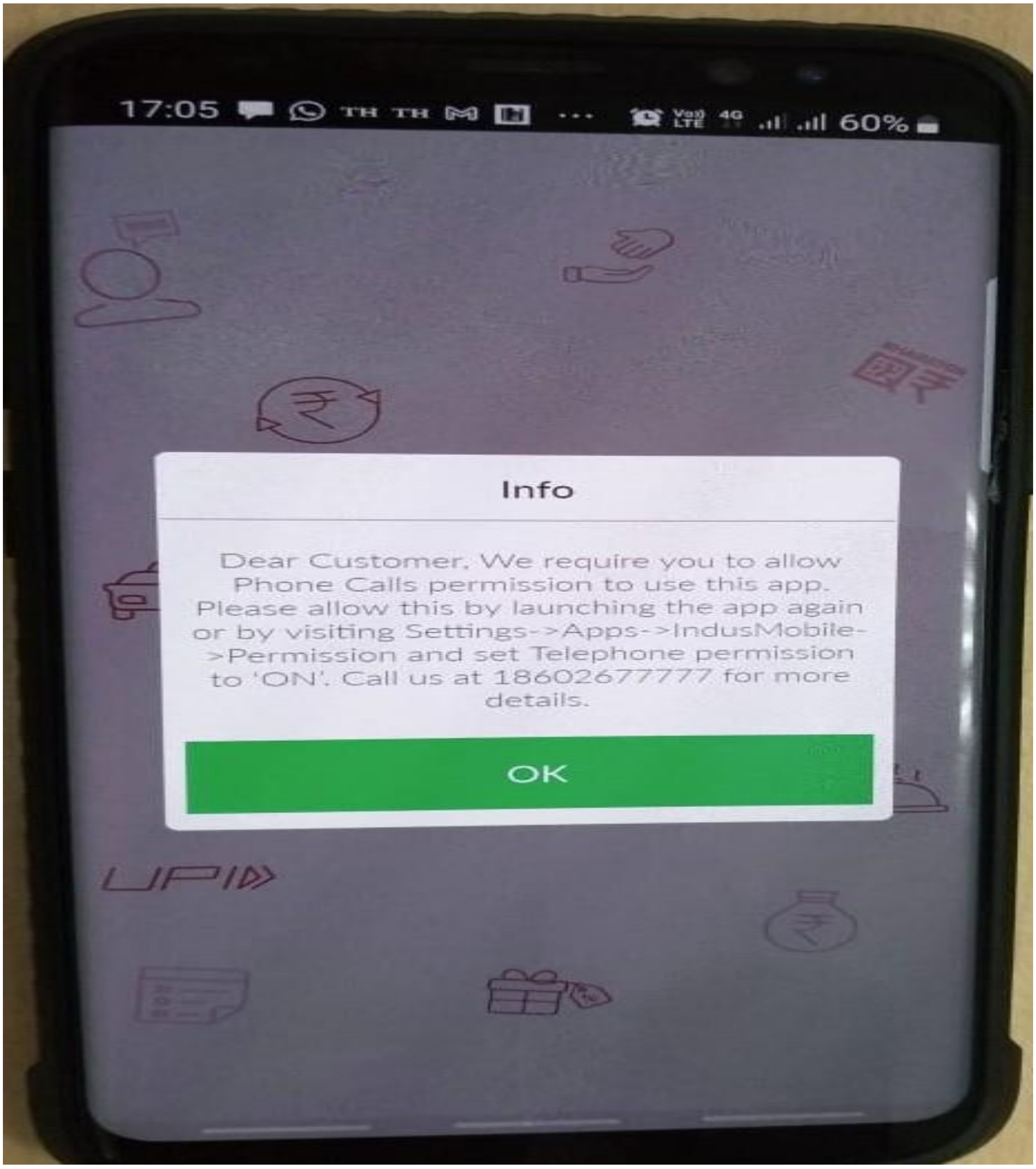
App permissions

IndusMobile

Camera	○
Contacts	○
Location	○
Storage	○
Telephone	●

Screenshot 12

Screenshot 12 shows the case where only one of the permissions sought by the app has been permitted and application was functional with only this permission. If we don't give this specific permission and application is opened for use then app behaves as displayed in **screenshot 13**. Screenshot 13 shows Application is informing that this permission is required to use this app.

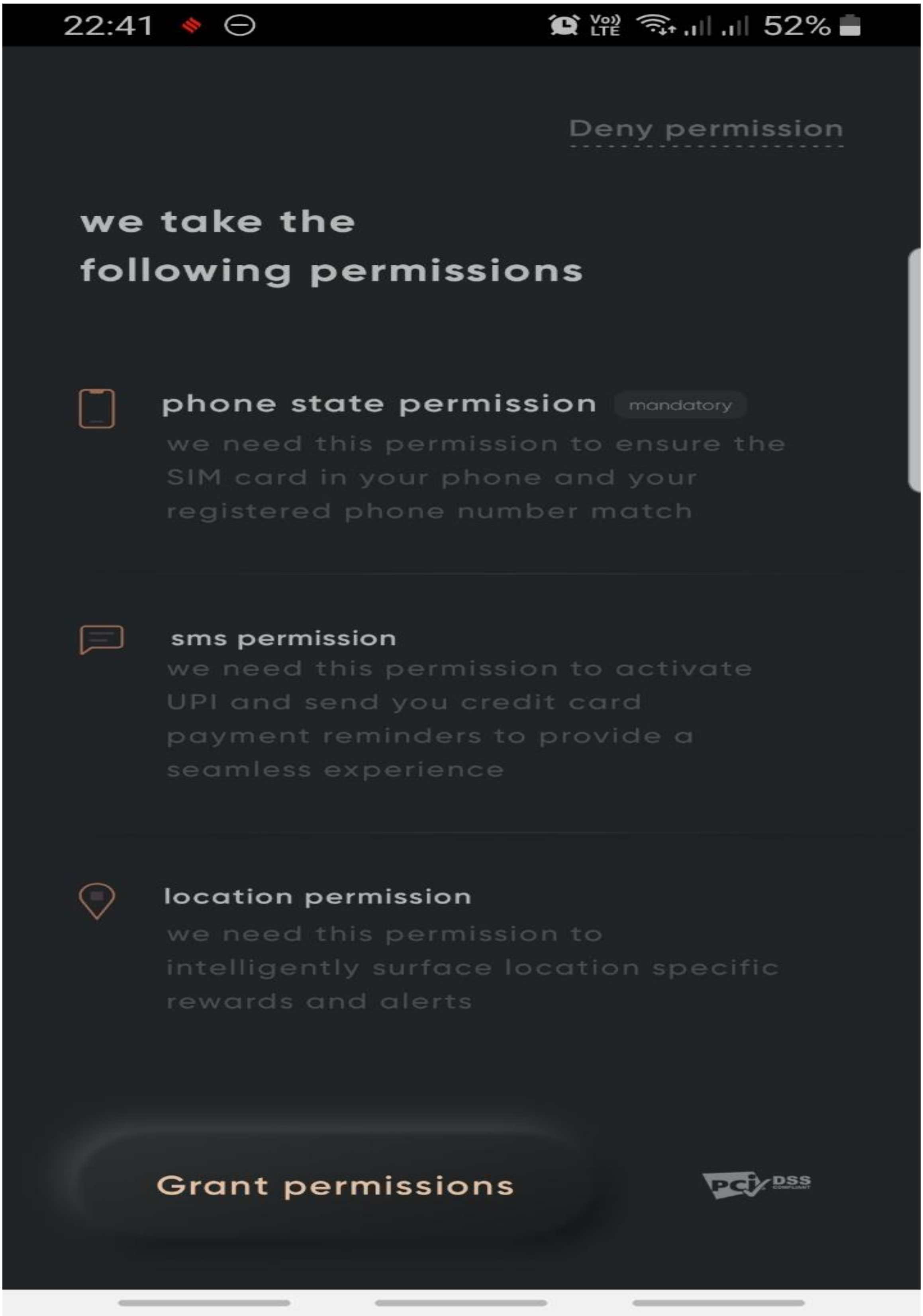


Dear Customer, We require you to allow Phone Calls permission to use this app. Please allow this by launching the app again or by visiting Settings->Apps->IndusMobile->Permission and set Telephone permission to 'ON'. Call us at 18602677777 for more details.

Screenshot 13

Case 3:

Screenshot 14 shows which of the permissions sought are mandatory and which are optional.



22:41 52%

Deny permission

we take the following permissions

phone state permission mandatory

we need this permission to ensure the SIM card in your phone and your registered phone number match

sms permission

we need this permission to activate UPI and send you credit card payment reminders to provide a seamless experience

location permission

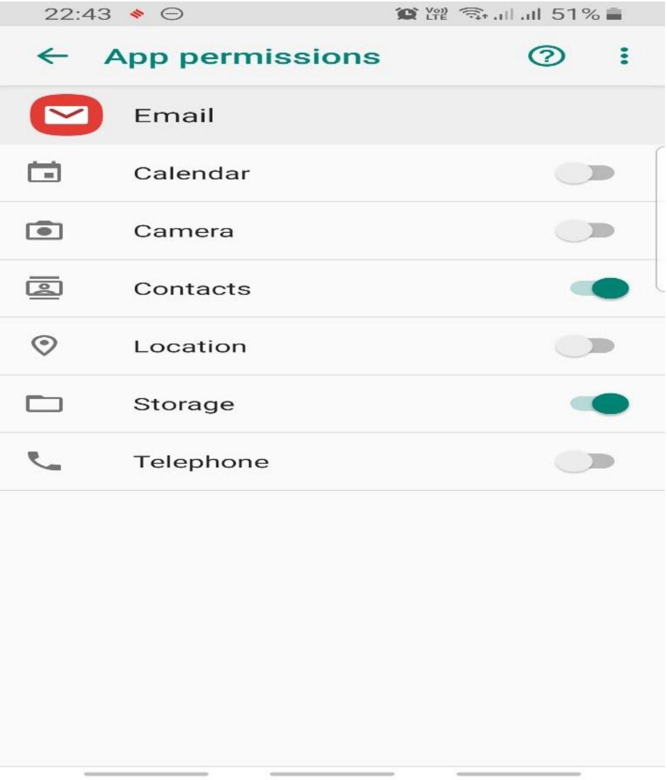
we need this permission to intelligently surface location specific rewards and alerts

Grant permissions

Screenshot 14

Case 4:

Now let us consider example of pre-installed applications. Screenshot 15 shows a pre-installed application



Email

Calendar ○

Camera ○

Contacts ●

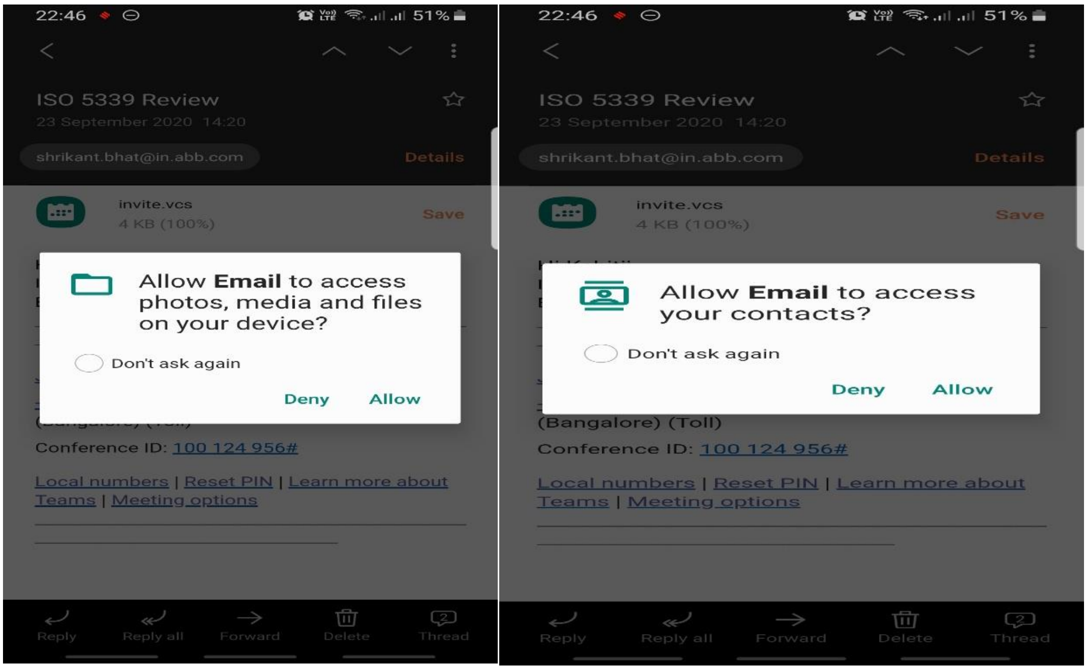
Location ○

Storage ●

Telephone ○

Screenshot 15

Permission shown in screnshot 15 are mandatorily required this came to notice only when, after denying permissions user tried to run app. After denying permissions user was able to view/read emails however was unable to send email or download the attahcments. The messages apearing when permission have been denied and user is trying to view/read/send emails or download the attahcments of the emails are shown in screenshot 16.



ISO 5339 Review
23 September 2020 14:20
shrikant.bhat@in.abb.com Details

invite.vcs
4 KB (100%) Save

Allow **Email** to access photos, media and files on your device?

○ Don't ask again

Deny Allow

(Bangalore) (Toll)
Conference ID: 100 124 956#
Local numbers | Reset PIN | Learn more about Teams | Meeting options

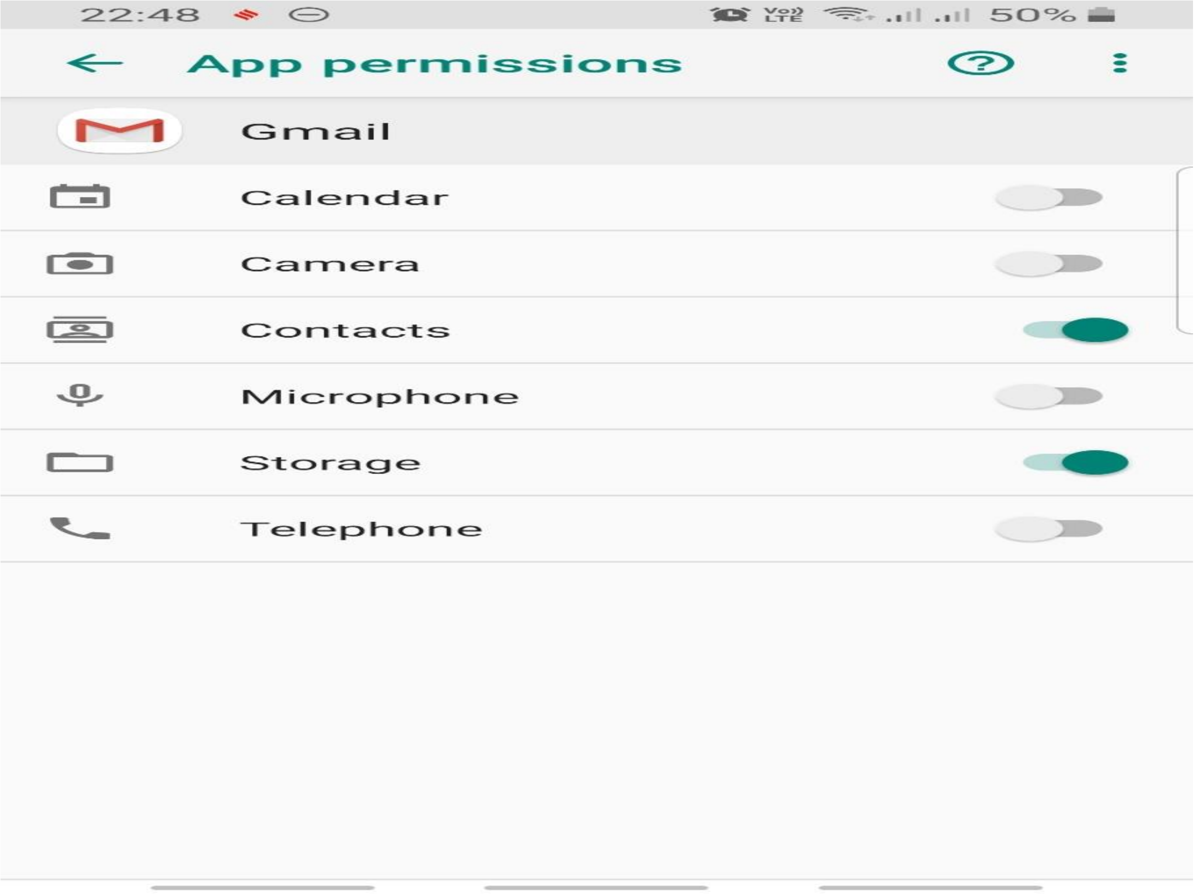
Allow **Email** to access your contacts?

○ Don't ask again

Deny Allow

Screenshot 16

Another similar application also requires same permissions as shown in screenshot 17:



App permissions

Gmail

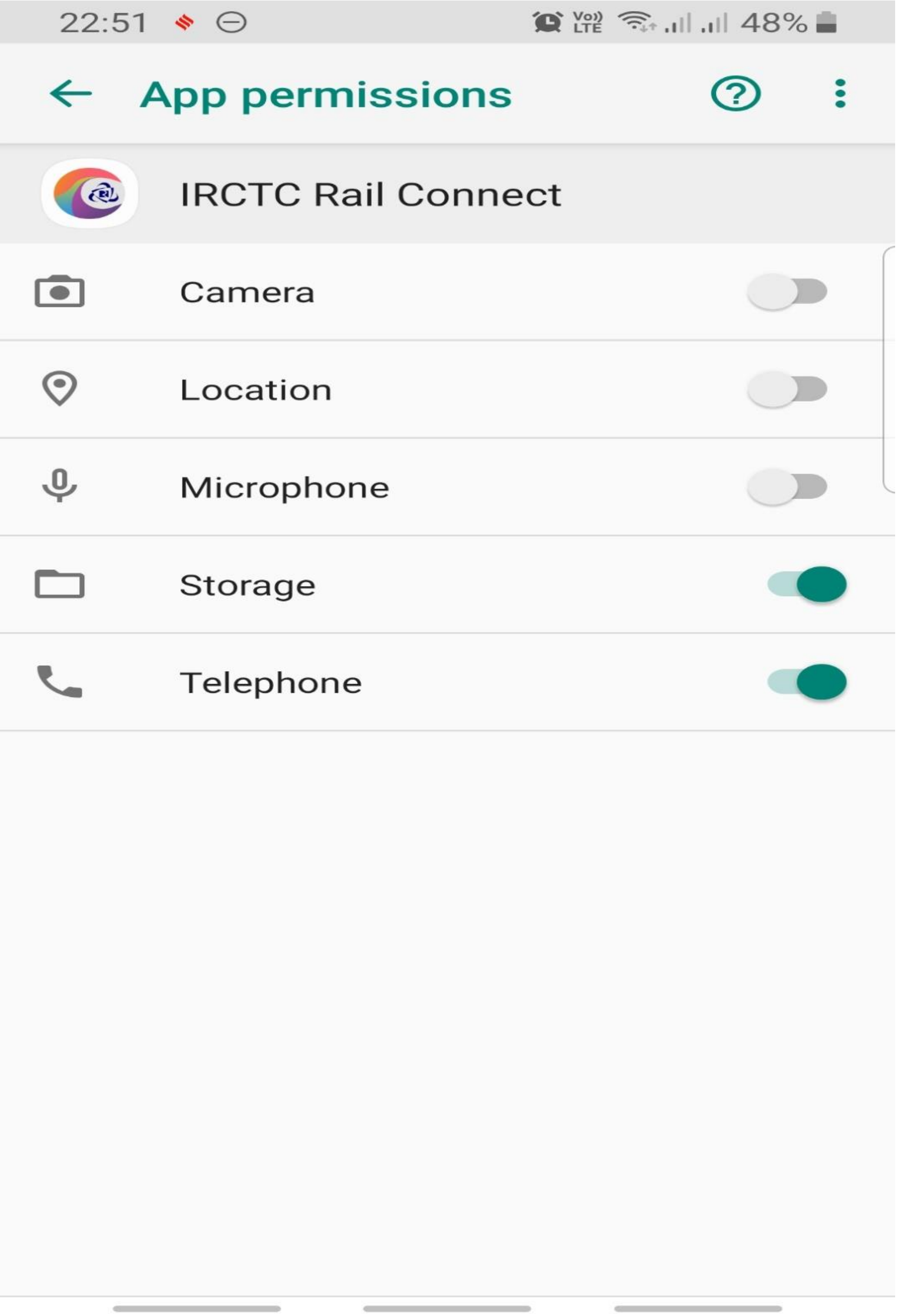
Calendar	○
Camera	○
Contacts	●
Microphone	○
Storage	●
Telephone	○

Screenshot 17

It shows that applications performing email functions require only storage and contacts permission for proper/intended function. This information should be informed to the user as and when application is used for the first time and also at all other times, if user want to know to check which permission is mandatory and which is optional.

Case 5:

Let us take another example of the application. Permissions given as shown in screenshot 18 seems to be mandatorily required permissions but it is not mentioned specifically.



22:51 48%

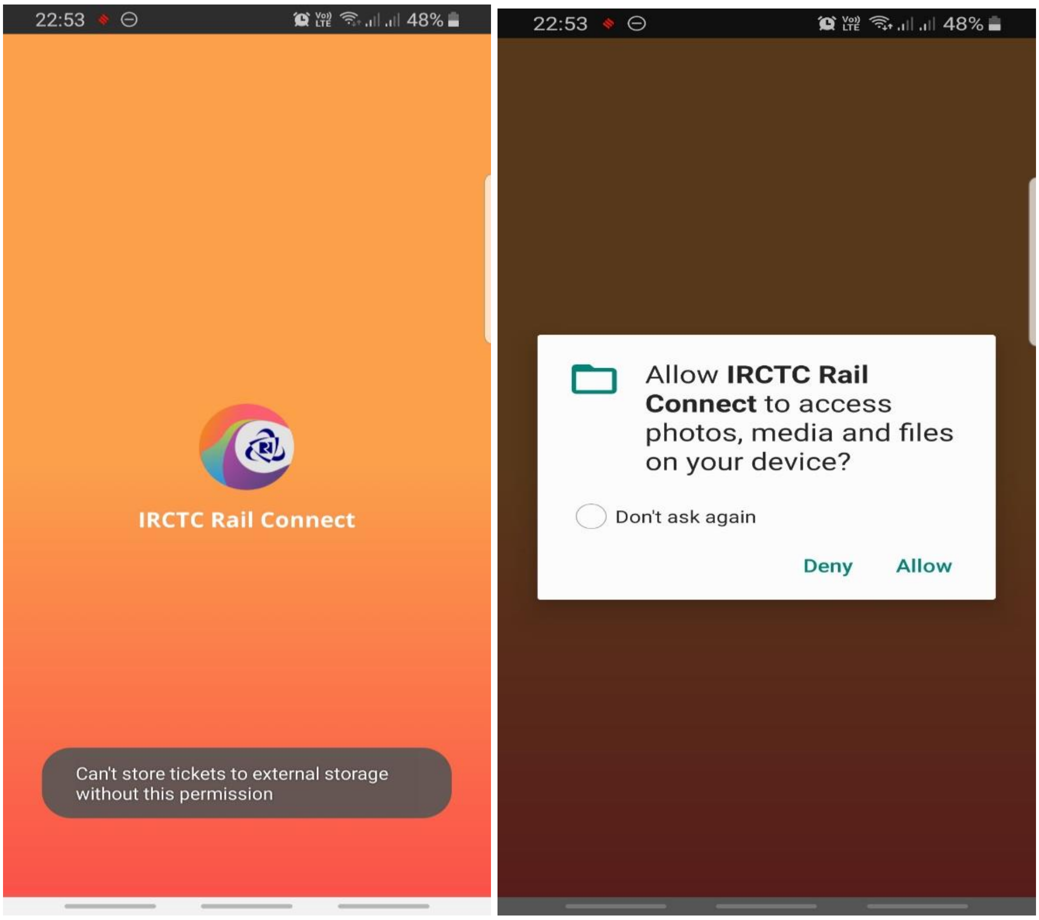
App permissions

IRCTC Rail Connect

Camera	○
Location	○
Microphone	○
Storage	●
Telephone	●

Screenshot 18

When permissions are denied and user tries to use the application at that time messages as shown in screenshot 19 & 20 appear and that to for a very brief moment and at that time it displays why the permission is required.

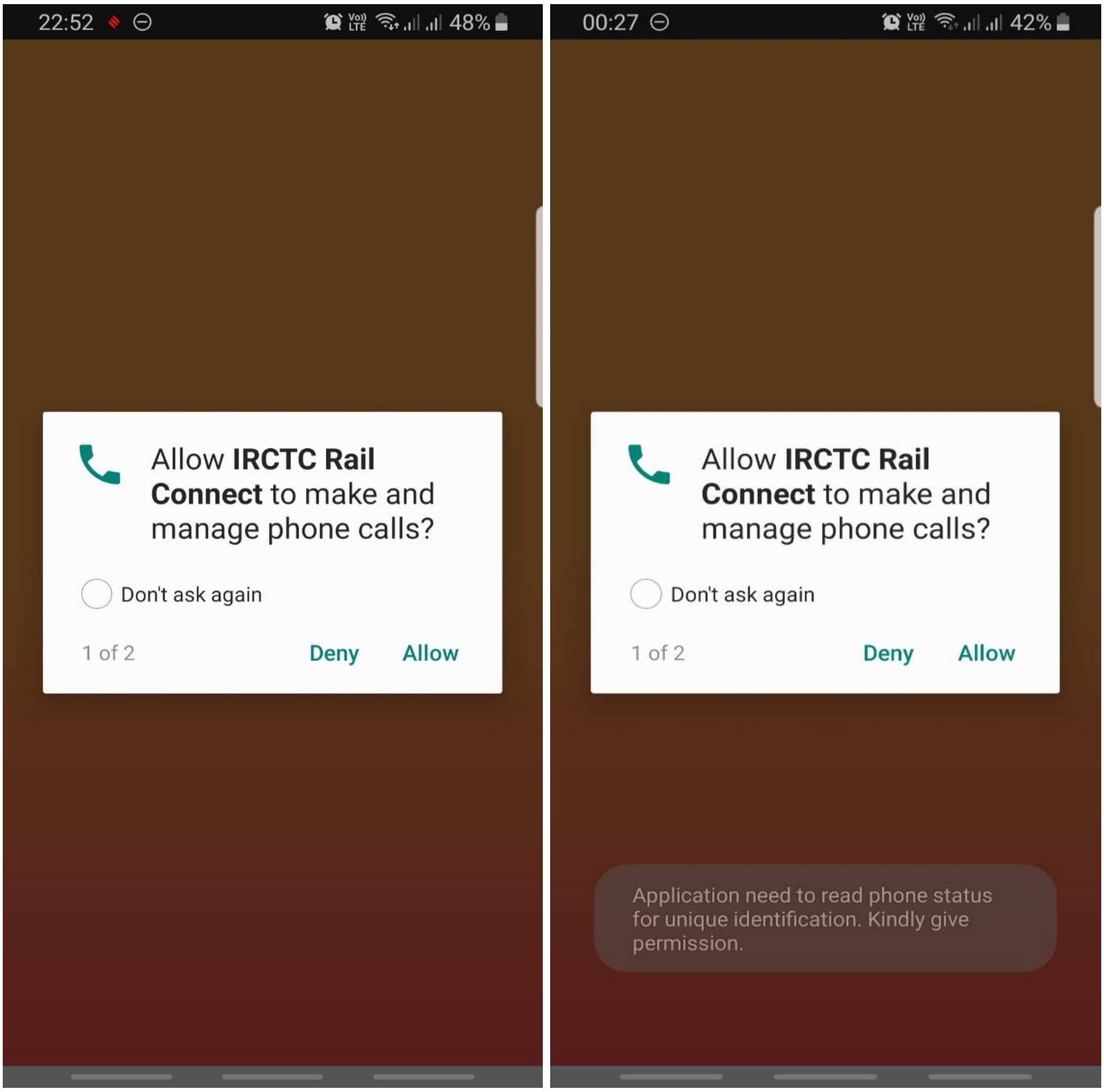


Can't store tickets to external storage without this permission

Allow **IRCTC Rail Connect** to access photos, media and files on your device?

○ Don't ask again

Screenshot 19



22:52 48%

Allow **IRCTC Rail Connect** to make and manage phone calls?

○ Don't ask again

1 of 2 Deny Allow

00:27 42%

Allow **IRCTC Rail Connect** to make and manage phone calls?

○ Don't ask again

1 of 2 Deny Allow

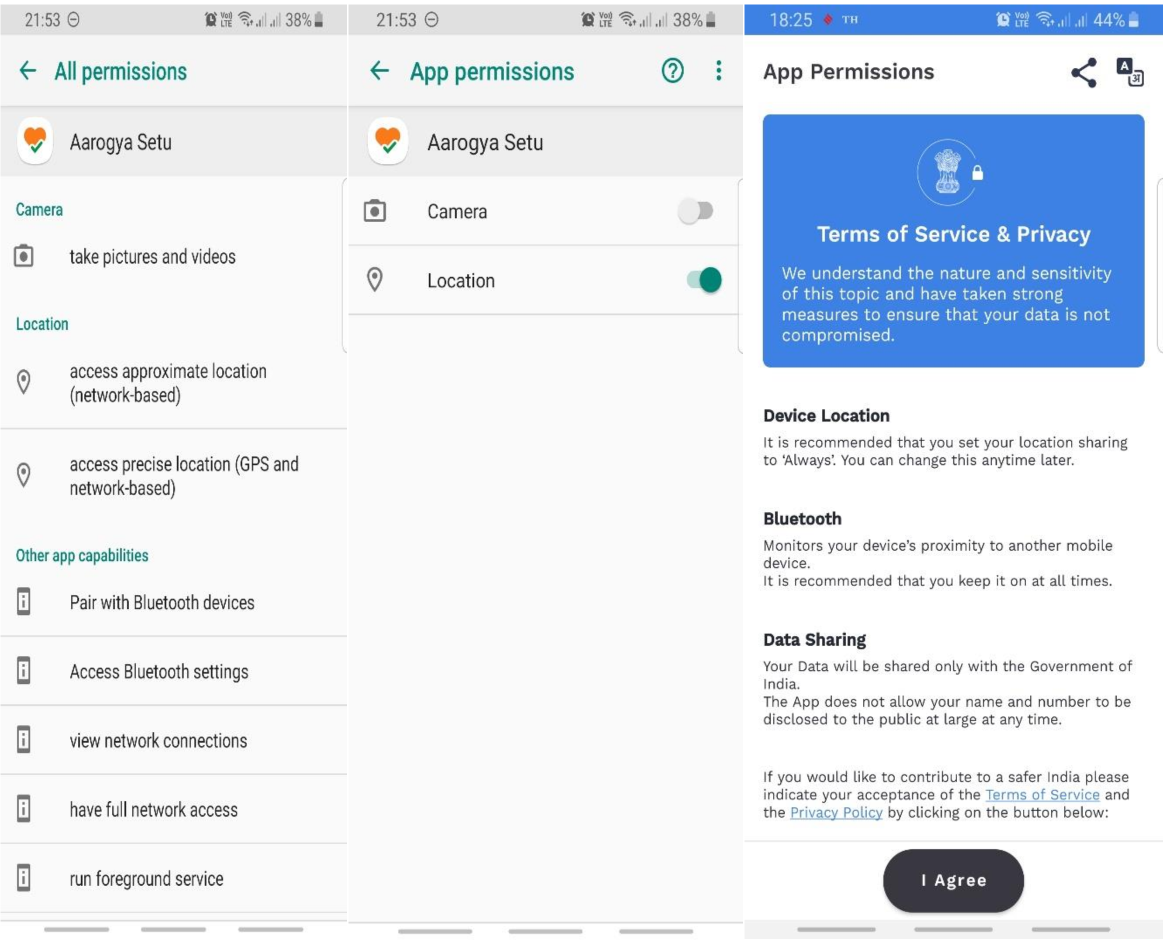
Application need to read phone status for unique identification. Kindly give permission.

Screenshot 20

From the above cases it emerges that not all permissions are mandatory some are optional.

6.5 Other app capabilities – Type 2 Permissions

Different applications have different 'other app capabilities' as mentioned at 6.3.2. Some of the Type 2 permissions are linked with Type 1 permissions and in that sense, user may be aware about those permissions but this is not always the case. Some of the app capabilities are benign like 'install shortcuts'. Some of the app capabilities like, 'Pair with Bluetooth devices' have potential to affect privacy of user as after paring app may share data. App shall always seek permissions to use 'other app capabilities' and ideally is should be like Type 1 Permissions. Refer screenshot 21 which shows an example where an application is using 'Pair with Bluetooth devices' by seeking explicit permission.



21:53 38%

All permissions

Aarogya Setu

Camera

take pictures and videos

Location

access approximate location (network-based)

access precise location (GPS and network-based)

Other app capabilities

Pair with Bluetooth devices

Access Bluetooth settings

view network connections

have full network access

run foreground service

21:53 38%

App permissions

Aarogya Setu

Camera

Location

18:25 44%

App Permissions

Terms of Service & Privacy

We understand the nature and sensitivity of this topic and have taken strong measures to ensure that your data is not compromised.

Device Location

It is recommended that you set your location sharing to 'Always'. You can change this anytime later.

Bluetooth

Monitors your device's proximity to another mobile device.
It is recommended that you keep it on at all times.

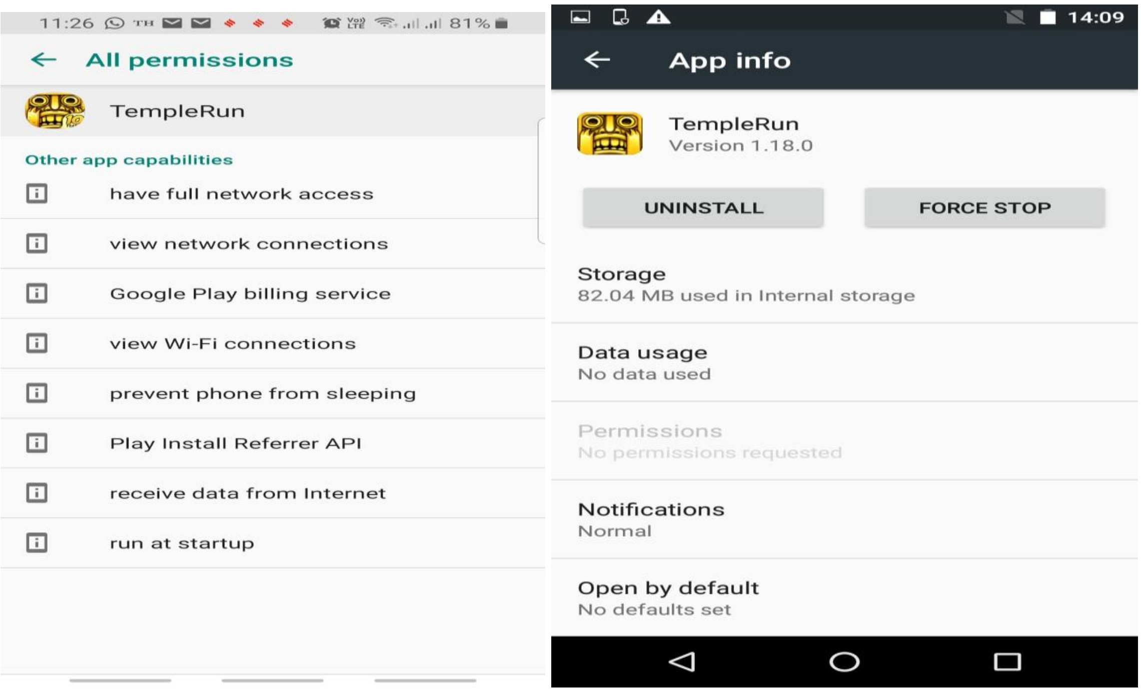
Data Sharing

Your Data will be shared only with the Government of India.
The App does not allow your name and number to be disclosed to the public at large at any time.

If you would like to contribute to a safer India please indicate your acceptance of the Terms of Service and the Privacy Policy by clicking on the button below:

I Agree

Screenshot 21



11:26 81%

All permissions

TempleRun

Other app capabilities

have full network access

view network connections

Google Play billing service

view Wi-Fi connections

prevent phone from sleeping

Play Install Referrer API

receive data from Internet

run at startup

14:09

App info

TempleRun
Version 1.18.0

UNINSTALL

FORCE STOP

Storage
82.04 MB used in Internal storage

Data usage
No data used

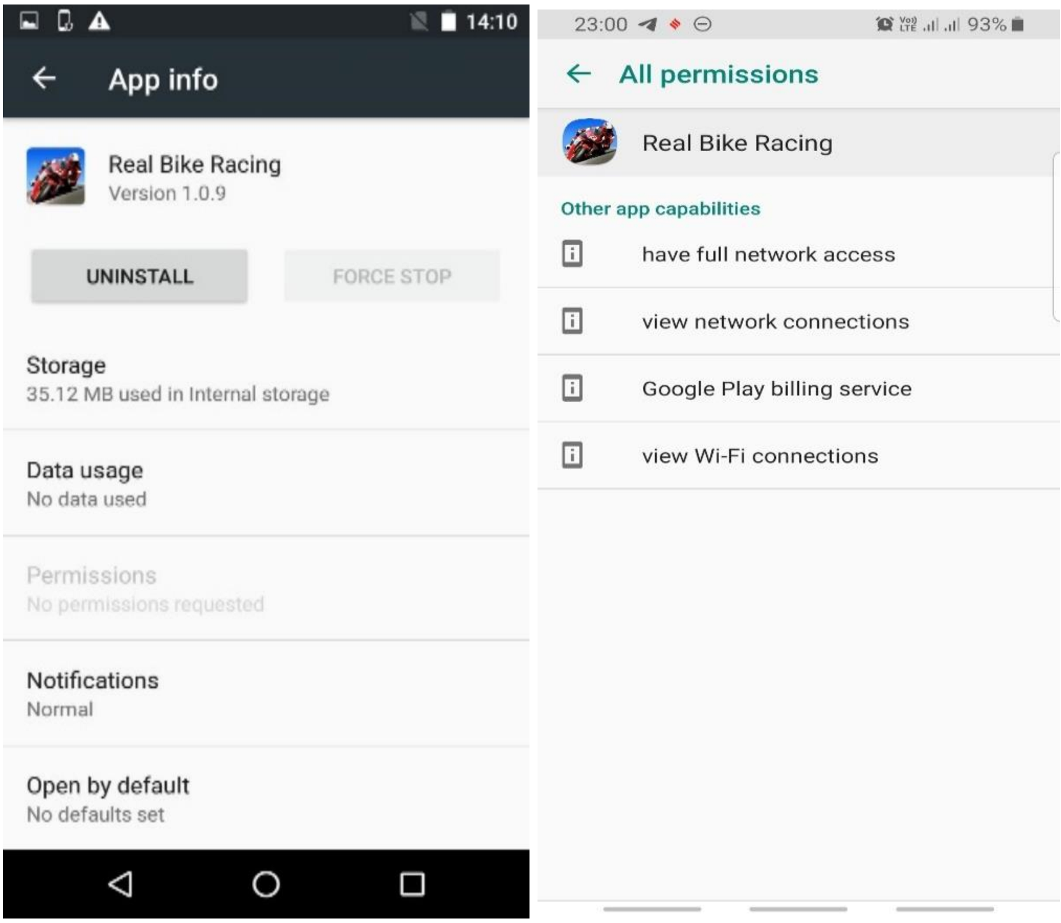
Permissions
No permissions requested

Notifications
Normal

Open by default
No defaults set

Screenshot 22

There are many applications which do not require any Type 1 permissions and still function properly and have many 'other app capabilities'. [Refer screenshot 22 & 23].



Real Bike Racing
Version 1.0.9

Storage
35.12 MB used in Internal storage

Data usage
No data used

Permissions
No permissions requested

Notifications
Normal

Open by default
No defaults set

Real Bike Racing

Other app capabilities

have full network access

view network connections

Google Play billing service

view Wi-Fi connections

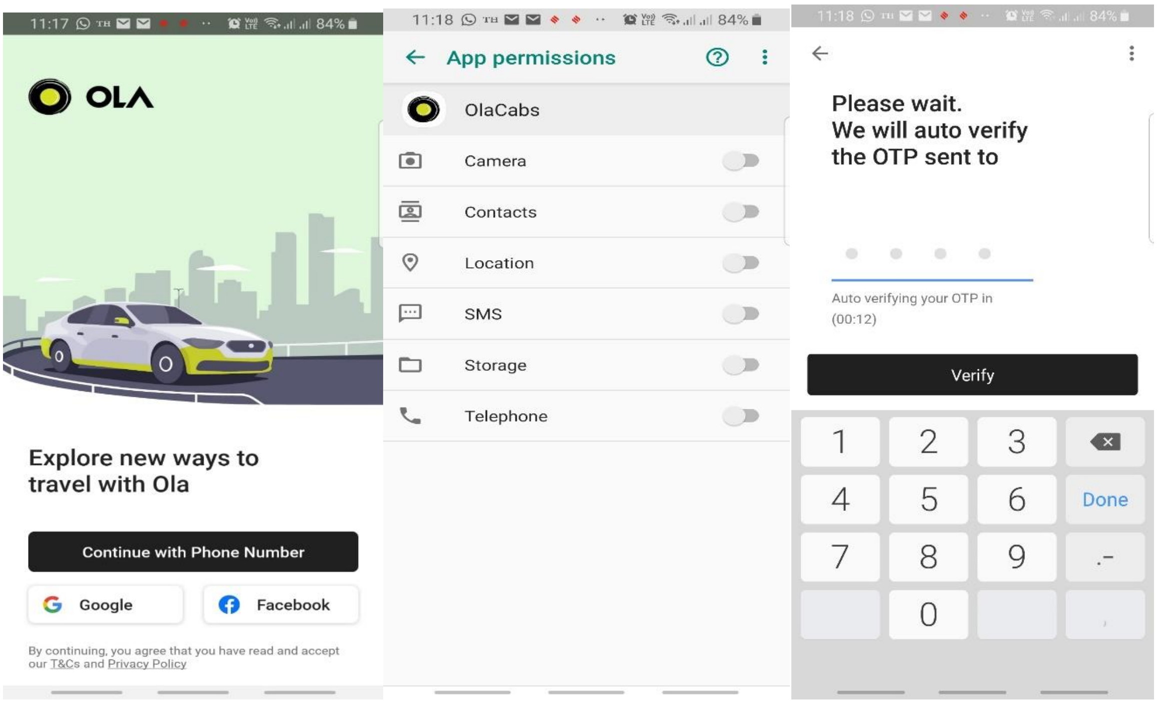
Screenshot 23

From the study it has been found that apps neither seek specific permission w.r.t 'other app capabilities' nor specifically inform the purpose and the kind of functions/capabilities which that app can do without user's permission. Any capabilities which lead to access, processing of user data shall be used only after consent of user.

6.6USE CASES

Case 1

An application (1) was downloaded. Application asked to login to as shown in screenshot 24. Before login no permission was provided to applications [Refer screenshot 24]. Still application is auto verifying the OTP and possible explanation of auto-verifying OTP seems to be through access to SMS for which no specific permission was asked.



Explore new ways to travel with Ola

By continuing, you agree that you have read and accept our T&Cs and Privacy Policy

App permissions

OlaCabs

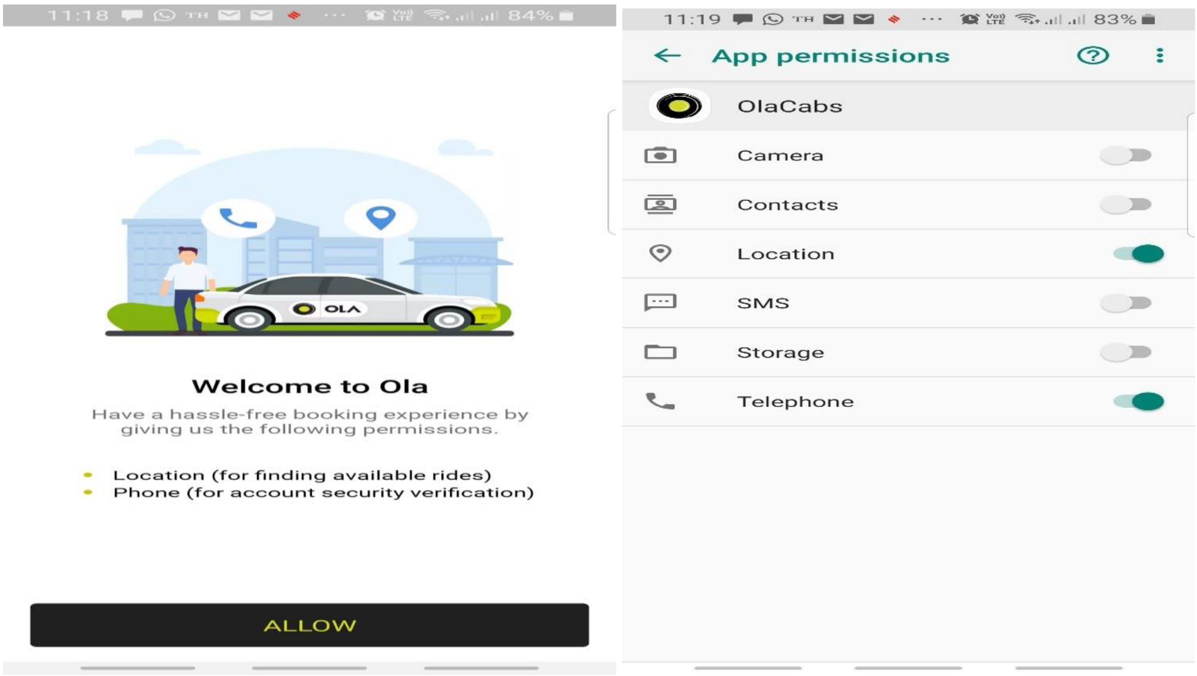
Camera	○
Contacts	○
Location	○
SMS	○
Storage	○
Telephone	○

Please wait.
We will auto verify
the OTP sent to

Auto verifying your OTP in (00:12)

Screenshot 24

After login application seeks permission for location and phone, if allowed app could be used for its intended function [refer screenshot 25]



Welcome to Ola

Have a hassle-free booking experience by giving us the following permissions.

- Location (for finding available rides)
- Phone (for account security verification)

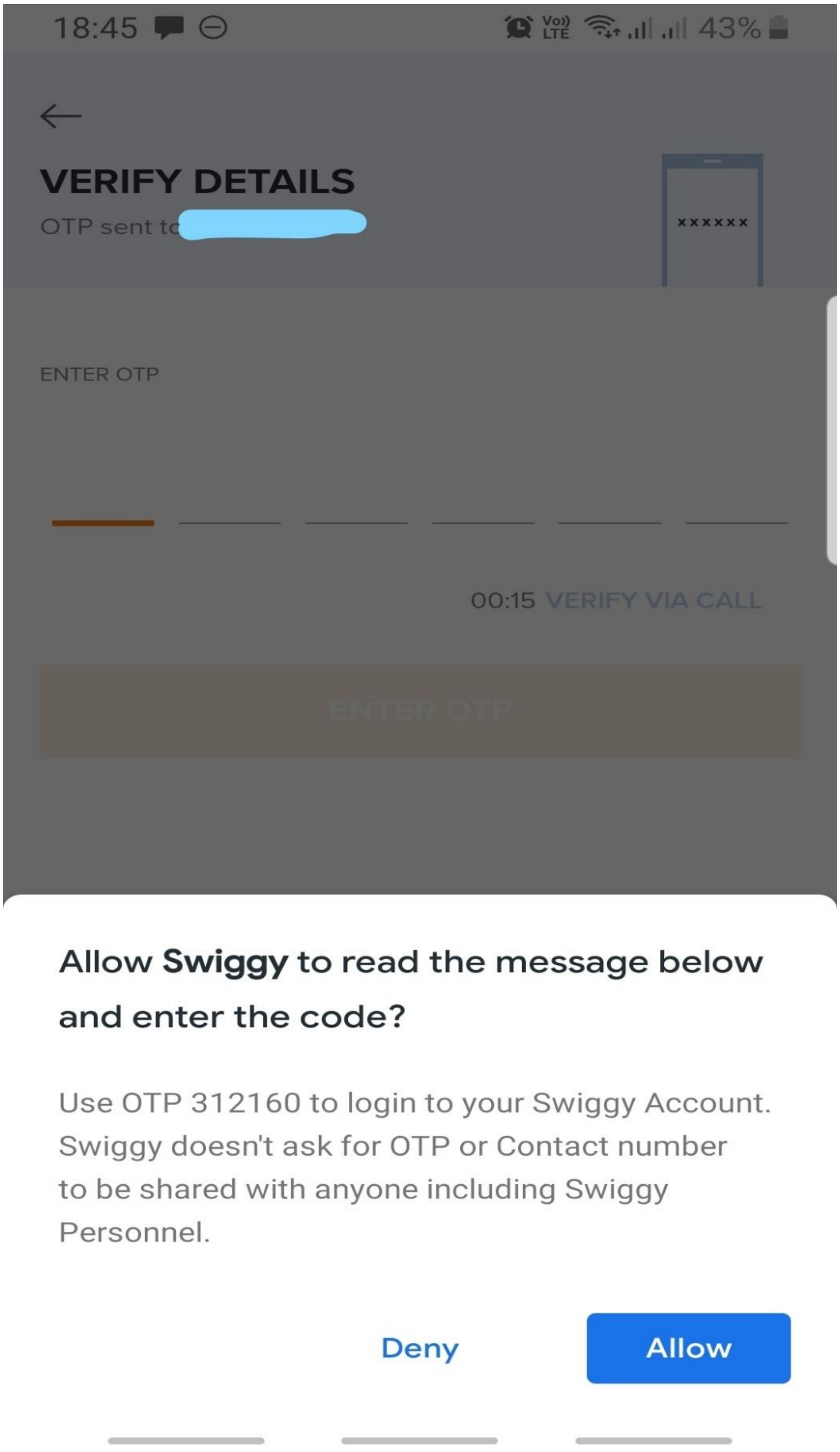
App permissions

OlaCabs

Camera	○
Contacts	○
Location	●
SMS	○
Storage	○
Telephone	●

Screenshot 25

Application (1) should have sought specific permission to read SMS for verification purpose only as done by another application (2) [refer screenshot 26].



VERIFY DETAILS

OTP sent to [redacted]

ENTER OTP

00:15 VERIFY VIA CALL

ENTER OTP

Allow **Swiggy** to read the message below and enter the code?

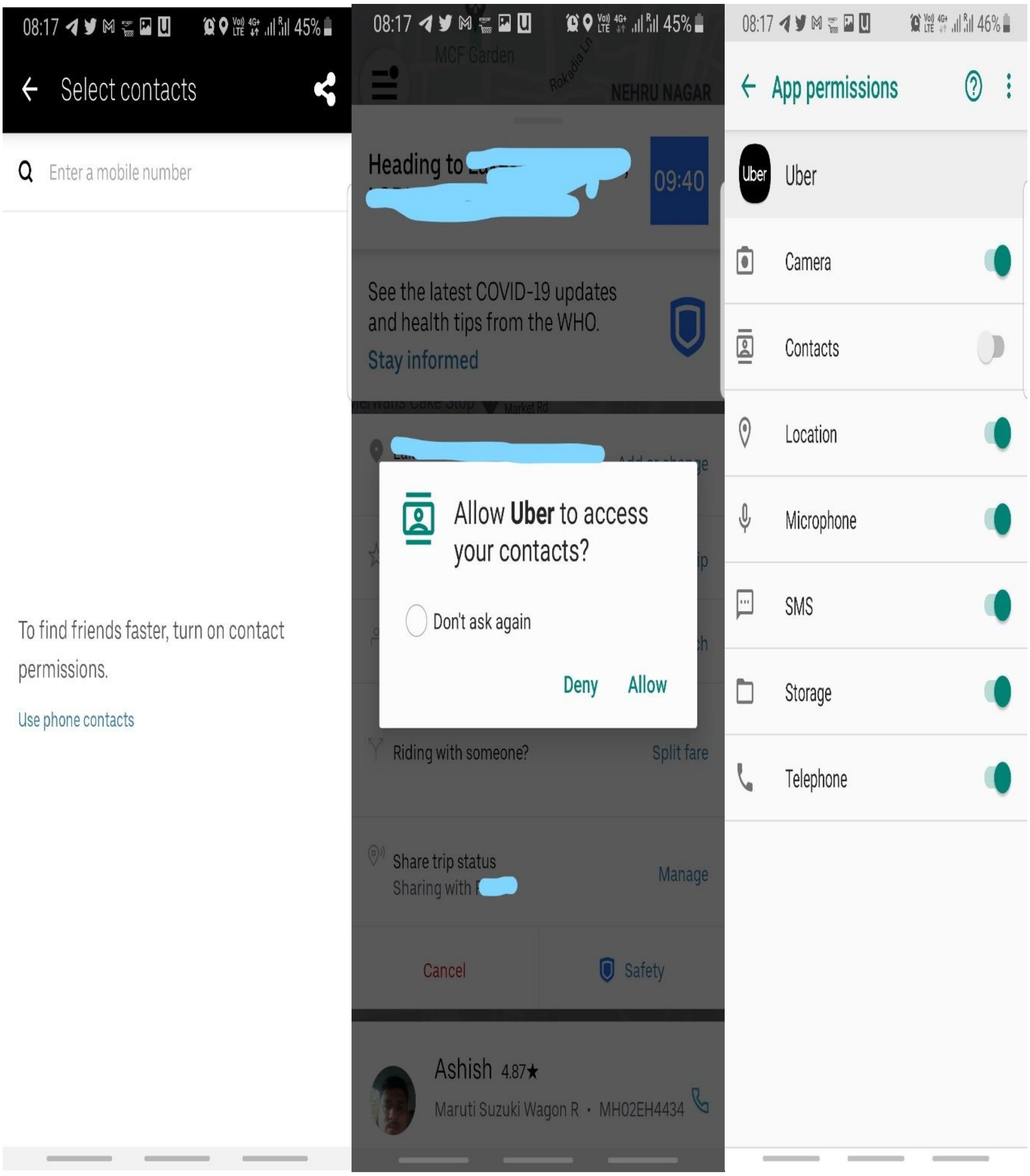
Use OTP 312160 to login to your Swiggy Account. Swiggy doesn't ask for OTP or Contact number to be shared with anyone including Swiggy Personnel.

Screenshot 26

Case 2

During usage of an application. User tried to share his trip details with someone and application sought permission to access contacts. Application was denied the permission to access contacts and mobile number was entered manually for sharing trip details. As application was not provided access to contacts hence ideally application should not be aware of the name of contact However, still application display the name of contact with whom trip details were shared [refer screenshot 27].

Only possible explanation of this seems to be that application is accessing contacts either indirectly through telephone permission or is accessing contacts without user's permission. It was found that even telephone permission for this app has not permission to - read phone numbers[refer screenshot 28].



08:17 45%

Select contacts

Enter a mobile number

To find friends faster, turn on contact permissions.

Use phone contacts

08:17 45%

MCF Garden

Rokadia Ln

NEHRU NAGAR

Heading to [redacted]

09:40

See the latest COVID-19 updates and health tips from the WHO.

Stay informed

[redacted]

Add or change

Allow **Uber** to access your contacts?

○ Don't ask again

Deny Allow

Riding with someone? Split fare

Share trip status

Sharing with [redacted]

Manage

Cancel

Safety

Ashish 4.87★

Maruti Suzuki Wagon R • MH02EH4434

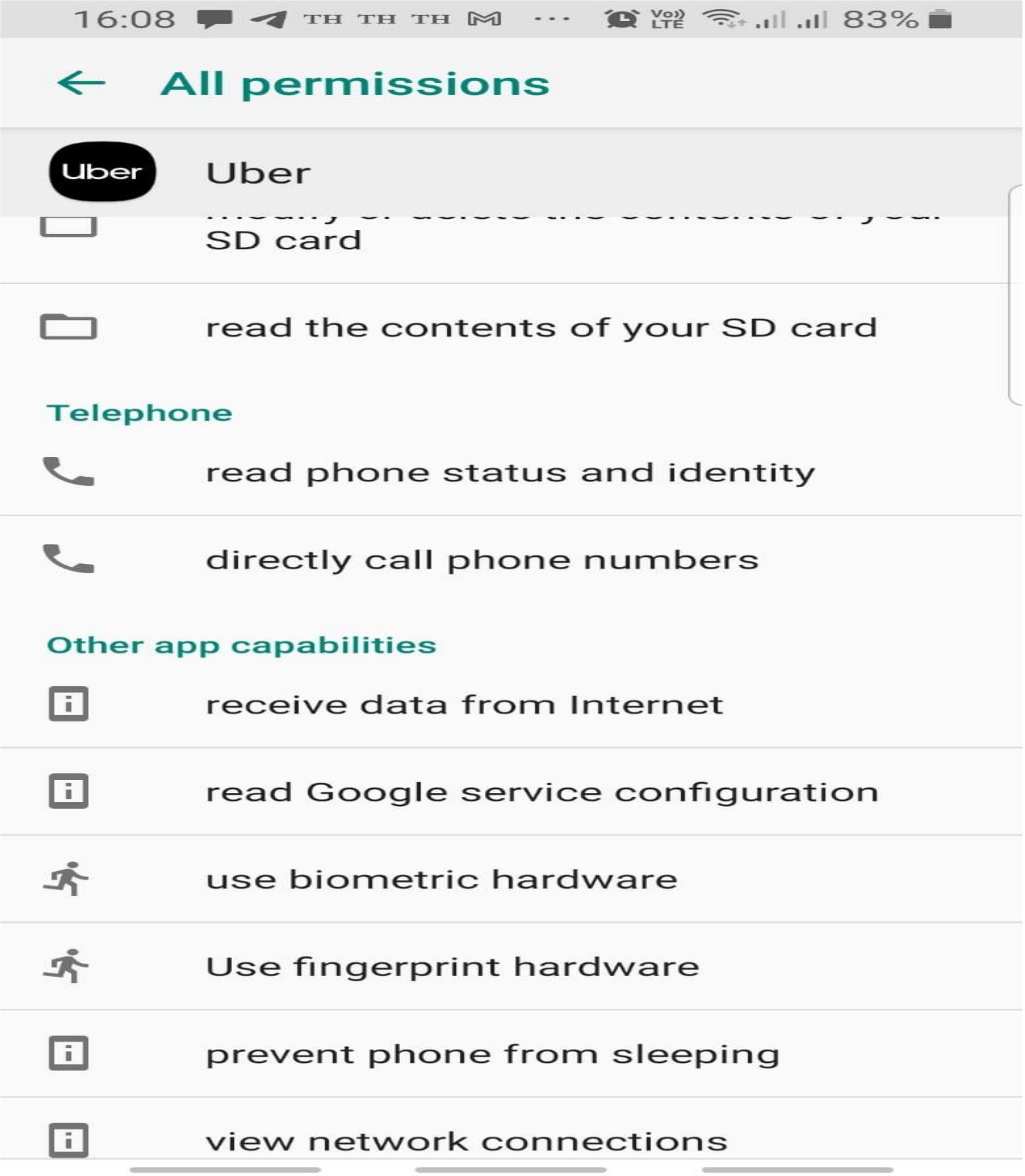
08:17 46%

App permissions

Uber

Camera	On
Contacts	Off
Location	On
Microphone	On
SMS	On
Storage	On
Telephone	On

Screenshot 27



16:08 83%

All permissions

Uber

SD card

read the contents of your SD card

Telephone

read phone status and identity

directly call phone numbers

Other app capabilities

receive data from Internet

read Google service configuration

use biometric hardware

Use fingerprint hardware

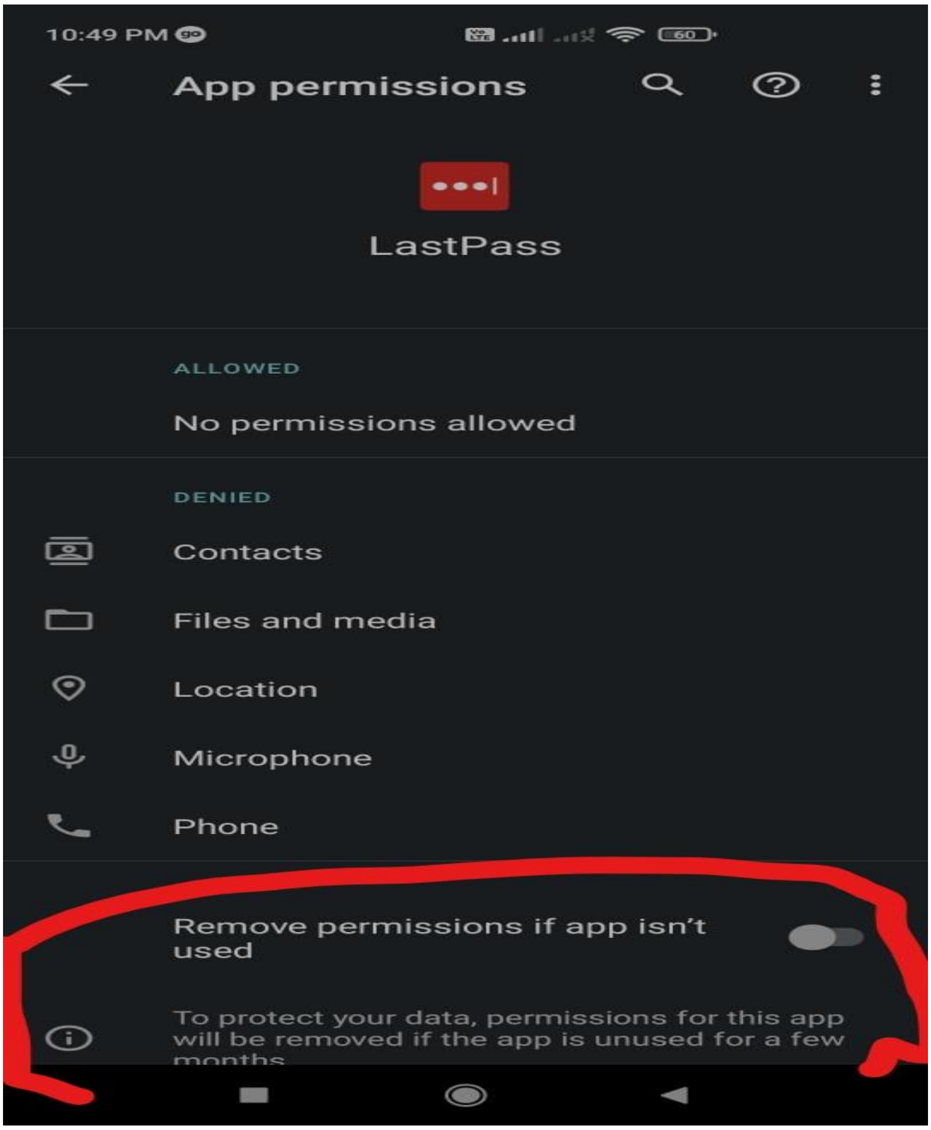
prevent phone from sleeping

view network connections

Screenshot 28

CASE 3
During the study some features came to notice which should be used by all mobile phones.

Remove permissions if app is not used: Many a times we download an application and then use it once or twice but do not uninstall the application. This feature would automatically deny all permissions if we do not use application for a certain period. [refer screenshot 29].



App permissions

LastPass

ALLOWED

No permissions allowed

DENIED

Contacts

Files and media

Location

Microphone

Phone

Remove permissions if app isn't used

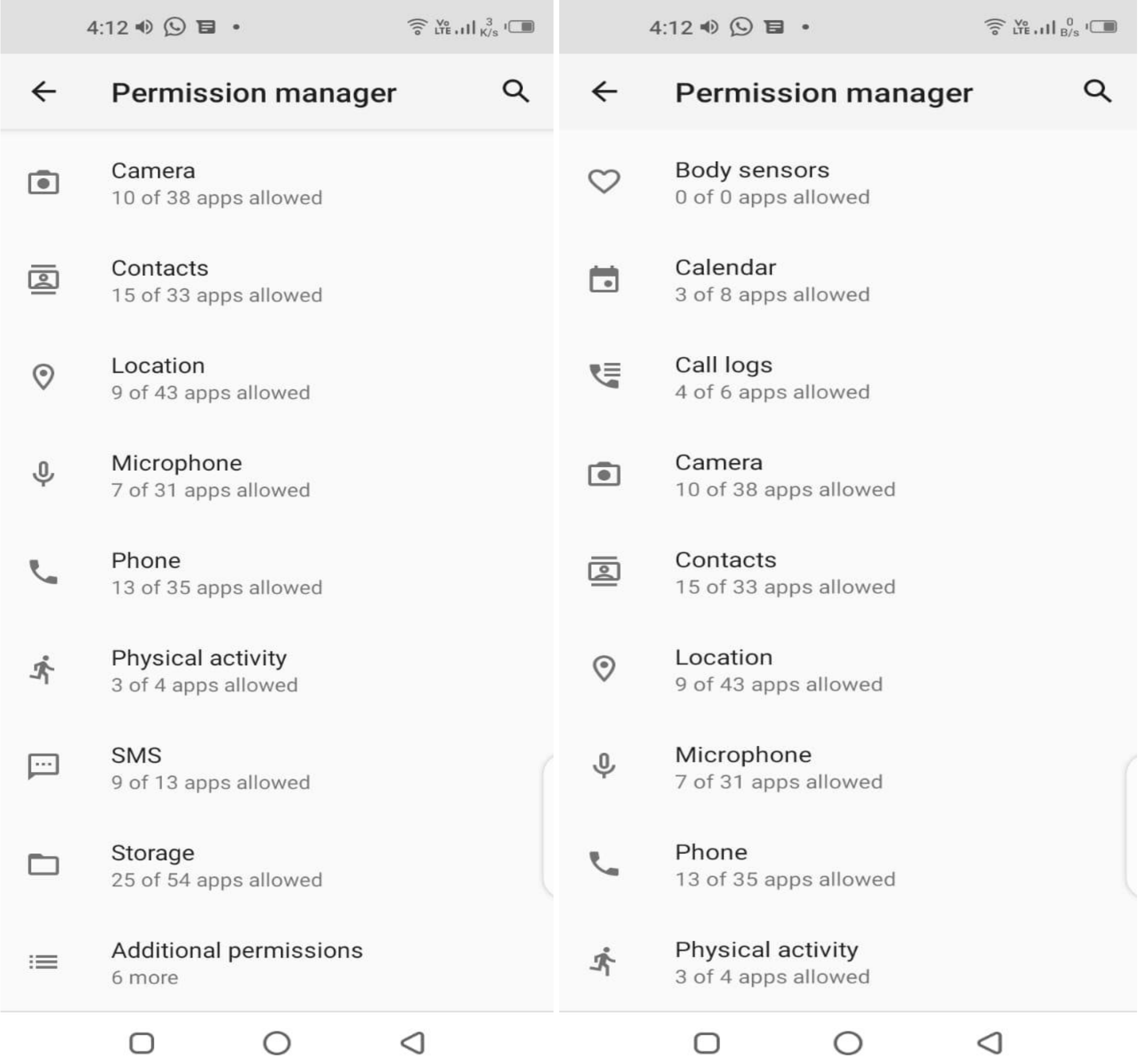
To protect your data, permissions for this app will be removed if the app is unused for a few months

Screenshot 29

Permissions manager

Permission manager is useful feature which provides important information to user like [refer screenshot 30]

a) permissions sought by different applications,
b) number of applications allowed a specific permission.



4:12

Permission manager

Camera
10 of 38 apps allowed

Contacts
15 of 33 apps allowed

Location
9 of 43 apps allowed

Microphone
7 of 31 apps allowed

Phone
13 of 35 apps allowed

Physical activity
3 of 4 apps allowed

SMS
9 of 13 apps allowed

Storage
25 of 54 apps allowed

Additional permissions
6 more

4:12

Permission manager

Body sensors
0 of 0 apps allowed

Calendar
3 of 8 apps allowed

Call logs
4 of 6 apps allowed

Camera
10 of 38 apps allowed

Contacts
15 of 33 apps allowed

Location
9 of 43 apps allowed

Microphone
7 of 31 apps allowed

Phone
13 of 35 apps allowed

Physical activity
3 of 4 apps allowed

Screenshot 30

7 Recommendations

- All mobile applications shall indicate which of the permissions are mandatory and which are optional.
- A short brief of the specific need of the permission shall be mentioned.
- In case application uses ‘other app capabilities’ which could lead to access, processing of personal data and could anyway affect the Privacy then this should be only after seeking specific permission
- Before user download an application, user should be mandatorily shown Privacy policy and privacy policy should be simple enough for ease of understanding of user.
- A standard for guidelines which can help application provider/developers to inform the clear and concise reason/need of the permission can be considered.